FGV DIREITO RIO

Thiago Bottino
Daniel Vargas
Fernanda Prates
COORDENADORES

SEGURANÇA PÚBLICA NA ERA DO BIG DATA

Mapeamento e diagnóstico da implementação de novas tecnologias no combate à criminalidade

PESQUISADORES

BIANCA KREMER • VICTORIA DE CASTRO PIRES • SAMUEL RODRIGUES DE OLIVEIRA • LUCAS KRAUSE • RAKEL DUQUE • ANA CLARA JACCOUD • ANDRESSA MOTA • BRUNA CROSSETTI • HENRIQUE KORMAN • ISABELLA MARINS • JOÃO PEDRO VERBICARIO • PEDRO FREITAS

Edição produzida pela FGV Direito Rio
Praia de Botafogo, 190 | 13º andar
Rio de Janeiro | RJ | Brasil | CEP: 22250-900
55 (21) 3799-5445
www.fgv.br/direito-rio

Thiago Bottino
Daniel Vargas
Fernanda Prates
COORDENADORES

SEGURANÇA PÚBLICA NA ERA DO BIG DATA

Mapeamento e diagnóstico da implementação de novas tecnologias no combate à criminalidade

PESQUISADORES

BIANCA KREMER ▪ VICTORIA DE CASTRO PIRES ▪ SAMUEL RODRIGUES DE OLIVEIRA ▪ LUCAS KRAUSE ▪ RAKEL DUQUE ▪ ANA CLARA JACCOUD ▪ ANDRESSA MOTA ▪ BRUNA CROSSETTI ▪ HENRIQUE KORMAN ▪ ISABELLA MARINS ▪ JOÃO PEDRO VERBICARIO ▪ PEDRO FREITAS

FGV DIREITO RIO

EDIÇÃO FGV Direito Rio

Impresso no Brasil.
Fechamento da 1ª edição em junho de 2023

Este livro consta na Divisão de Depósito Legal da Biblioteca Nacional.

Este material, seus resultados e conclusões são de responsabilidade dos autores e não representam, de qualquer maneira, a posição institucional da Fundação Getulio Vargas / FGV Direito Rio.

Coordenação: Ludmilla Totinick, Christian Danniel e Victor Almeida
Capa e diagramação: Estúdio Castellani
1ª revisão: Filipe Castro
2ª revisão: Christian Danniel

Dados Internacionais de Catalogação na Publicação (CIP)
Ficha catalográfica elaborada pela Biblioteca Mario Henrique Simonsen/FGV

Segurança pública na era do big data [recurso eletrônico] : mapeamento e diagnóstico da implementação de novas tecnologias no combate à criminalidade / [coordenadores] Thiago Bottino, Daniel Vargas, Fernanda
Prates (coords). — Rio de Janeiro : FGV Direito Rio, 2023.
1 recurso online (200 p.) : PDF

Dados eletrônicos.
Inclui bibliografia.
ISBN 9786586060485

1. Segurança pública — Brasil — Inovações tecnológicas. 2. Tecnologia da informação — Aspectos sociais. 3. Criminalidade urbana — Brasil — Processamento de dados. 4. Big data. I. Amaral, Thiago Bottino do. II. Vargas, Daniel. III. Prates, Fernanda. IV. Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas.

CDD — 341.5514

Elaborada por Márcia Nunes Bacha — CRB-7/4403

Sumário

Introdução

A adoção de novas tecnologias nas investigações criminais vem ganhando espaço importante no campo da segurança pública. É possível observar a utilização progressiva de diferentes tipos de ferramentas tecnológicas no combate ao crime, tanto através da percepção nas ruas quanto pelas notícias transmitidas pelos principais veículos de comunicação do país. Contudo, ainda repousam dúvidas em relação às estratégias de implementação em curso, em perspectiva quantitativa e qualitativa.

No contexto de uma sociedade cada vez mais hiperconectada e movida a dados, a modernização dos aparatos de investigação tem gerado desafios às forças de segurança diante das implicações promovidas pelo mundo digital. De um lado, a necessidade premente de modelos modernos de investigação criminal e novas abordagens para a investigação e repressão de condutas impulsionadas pelas novas tecnologias. De outro, diferentes especialistas demonstram preocupação com a ausência de regulamentação jurídica sobre o uso de dados pessoais e de sistemas automatizados pelos órgãos de segurança pública, além de desconhecimento geral sobre os tipos de tecnologias adotadas, suas finalidades e extensão de uso.

Nesse sentido, buscamos com o presente estudo — realizado ao longo de dezoito meses por pesquisadores do Centro de Justiça e Sociedade da FGV Direito Rio — promover o mapeamento e a análise da utilização de novas tecnologias no âmbito da segurança pública no Brasil. Foram abordados estudos de caso específicos, tendo como objeto a utilização de tecnologias especialmente relevantes.

No intuito de identificar e analisar o panorama de implementação de novas tecnologias no enfrentamento à criminalidade no Brasil, a pesquisa se dedicou a duas atividades essenciais. A primeira: compilar e mapear as principais

práticas tecnológicas inovadoras adotadas pelas forças de segurança no cenário brasileiro, a partir de uma metodologia de cunho exploratório e análise documental de reportagens e publicações. A segunda: desenvolver um estudo de caso de metodologia qualitativa, com recorte na cidade do Rio de Janeiro, dedicado à percepção pessoal dos agentes de segurança pública lotados em diferentes órgãos da região, sobre os usos de tecnologias baseadas em dados em suas atividades laborais.

Buscou-se, assim, identificar e analisar as estratégias de implementação das novas ferramentas tecnológicas no combate ao crime, mapeando práticas inovadoras e examinando os desafios para sua consolidação, para compreender, através dos atores penais, de que maneira as novas tecnologias estão sendo integradas ao sistema de segurança e justiça.

O texto traz exemplos práticos de sua implementação a partir de um mapeamento nacional e das percepções pessoais dos agentes de segurança em um estudo de caso focado na cidade do Rio de Janeiro, traçando correlações entre os mapeamentos identificados e as narrativas dos policiais e órgãos de segurança pública, à luz de suas experiências vividas.

Em relação à metodologia de pesquisa, é possível classificá-la como uma pesquisa exploratória no que tange aos seus objetivos. Esse tipo de pesquisa objetiva proporciona maior familiaridade com o problema, a fim de torná-lo mais explícito ou de construir hipóteses. As pesquisas exploratórias:

> [...] têm como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a constituir hipóteses. Pode-se dizer que estas pesquisas têm como objetivo principal o aprimoramento de ideias [*sic*] ou a descoberta de intuições. Seu planejamento é, portanto, bastante flexível, de modo que possibilite a consideração dos mais variados aspectos relativos ao fato estudado. Na maioria dos casos, essas pesquisas envolvem: (a) levantamento bibliográfico; (b) entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado; e (c) análise de exemplos que estimulem a compreensão (Gil, 2002, p. 41).

Embora exista uma produção bibliográfica relativamente extensa sobre o uso de tecnologias baseadas em dados pelos órgãos de segurança pública em nível mundial, essa realidade não se verifica no Brasil, onde há poucos estudos teóricos que se debruçam com profundidade sobre o tema.

Nesse sentido, optou-se pela pesquisa empírica no presente estudo, a partir de dois eixos principais: o primeiro foi dedicado à análise documental de reportagens e publicações sobre o uso de tecnologias baseadas em dados por forças de segurança pública no Brasil, para fins de mapeamento e análise do conjunto de estratégias inovadoras em curso, enquanto o segundo tem foco nas entrevistas com agentes de segurança cujas experiências práticas possuem relação com o problema pesquisado. Foram entrevistados vinte e três agentes, lotados em diferentes órgãos: polícia militar (PM), polícia civil (PC), polícia federal (PF) e Ministério Público (MP).

As primeiras entrevistas realizadas serviram como ponto de partida para a segunda etapa da pesquisa, que consistiu no mapeamento de notícias sobre o uso de novas tecnologias pelos órgãos de segurança pública no Brasil. A partir das entrevistas, foram identificados alguns dos principais tipos de tecnologia empregados no país, com base na sua recorrência nas falas dos entrevistados. São eles: câmeras corporais (*bodycams*), drones, reconhecimento facial e reconhecimento óptico de caracteres (OCR) para leitura de placas veiculares.

Os apontamentos metodológicos da terceira etapa da pesquisa, que corresponde à análise qualitativa das entrevistas realizadas, será endereçada em momento posterior deste trabalho, em capítulo específico. Dedicaremos nossa atenção, por ora, à segunda etapa: o mapeamento de notícias sobre o uso de tecnologias baseadas em dados pelos órgãos de segurança pública no Brasil.

A pesquisa empírica no âmbito digital demanda, na maioria das vezes, o uso de técnicas inovadoras e processos mais eficazes na análise — observação e recolhimento — dos dados disponíveis nos meios digitais (Fragoso, Recuero e Amaral, 2011, p. 11). Segundo Serbena, em se tratando do desenvolvimento de análises que lidem com uma quantidade massiva de dados, a pesquisa manual se releva ilimitada ou, por vezes, impossível, de modo que os pesquisadores necessitarão utilizar técnicas computacionais para a análise dos dados; nesse contexto, a mineração de dados pode ser utilizada na pesquisa jurídica empírica. Nas palavras do autor:

> A mineração de dados é um ramo da Computação que teve início por volta de 1980. Ela surgiu primeiramente como ferramenta para a análise dos dados de grandes empresas e organizações, que no curso da sua atividade, acumulavam uma quantidade massiva de informação. A análise dos bancos de dados poderia fornecer informações que não estavam aparentes e

> que, uma vez conhecidas, poderiam otimizar e aumentar a performance da organização. Atualmente, com o aumento do trânsito de dados dos computadores para os celulares e dispositivos intermediários, como tablets, a mineração de dados é cada vez mais empregada como técnica de análise automática de informações e geração de conhecimento; como o próprio termo designa, trata-se de minerar os dados (Serbena, 2022, p. 53).

Nessa perspectiva, o *Media Cloud*, desenvolvido pelo Massachusetts Institute of Technology (MIT), é uma ferramenta de compilação de notícias que pode se revelar útil para explorar a cobertura de temas de interesse em veículos variados (National Democratic Institute, 2020), especialmente para os fins aqui empreendidos.

A ferramenta permite compilar dados de mais de cinquenta mil fontes de notícia ao redor do mundo em mais de vinte línguas, contribuindo para a análise, o compartilhamento e a visualização de informações sobre assuntos tratados na mídia sob três eixos principais: picos de interesse e de cobertura dos temas, análises de redes e a utilização de línguas *clusterizadas.*[1] De acordo com Hartmann *et al*., o *Media Cloud*:

> (...) constitui-se de uma plataforma para estudar ecossistemas de mídia, ou seja, as relações entre as instituições e os profissionais criadores de mídia — impressa e digital — e os cidadãos. Por meio do monitoramento programático de milhões de notícias, publicadas online ou transmitidas em canais de televisão, o sistema permite aos pesquisadores monitorar a disseminação de notícias, conceitos e memes, além de permitir a descoberta das redes de atores que pautam a mídia, através da genealogia das notícias. Também permite que se façam análises geográficas — através da identificação da cobertura midiática nas diversas regiões, e políticas, monitorando a abordagem específica dos diversos atores, politicamente identificados com as principais correntes partidárias, segundo os diversos temas de interesse, identificando-se vieses (Hartmann *et al*, 2015, p. 19).

---

1 "Cluster", em inglês, significa "grupo". Portanto, "clusterizar" nada mais é do que agrupar. Esse agrupamento, por sua vez, pode ser de um conjunto de dados, de clientes, de computadores ou o que mais for necessário. Assim, o termo é utilizado com mais frequência por desenvolvedores, profissionais de marketing, TI ou cientistas de dados, os quais recorrem à clusterização como forma de organizar dados ou segmentá-los. Cf. Clusterização: o que é, importância e aplicações. **Blog da Five Acts**. Disponível em: <https://www.fiveacts.com.br/clusterizacao/>. Acesso em: 04 ago. 2022.

Enquanto ferramenta computacional, o *Media Cloud* pode ser caracterizado como uma ferramenta de análise de conteúdo de fonte aberta (*open source*), que desempenha cinco funções básicas, a saber: a definição de fontes de mídia de interesse, a captura (*crawling*) contínua de notícias, a extração de características semânticas dos textos, como análise de assunto e de conteúdo, a construção de estatísticas sobre frequências de palavras através de processamento de linguagem natural e, finalmente, a análise dos resultados (Hartmann *et al*, 2015, p. 20).

Dentro da plataforma *Media Cloud*, utilizamos a ferramenta *Explorer* para realizar a pesquisa, que funciona da seguinte maneira: 1. Em primeiro lugar, inserem-se os termos de pesquisa (*Enter search terms*); 2. Selecionam-se as "mídias" (*Select your media*), isto é, os veículos ou fontes em que os termos serão pesquisados; 3. Em seguida, seleciona-se o universo temporal da pesquisa ("*Enter dates*"). A Figura 1 ilustra o funcionamento da ferramenta:

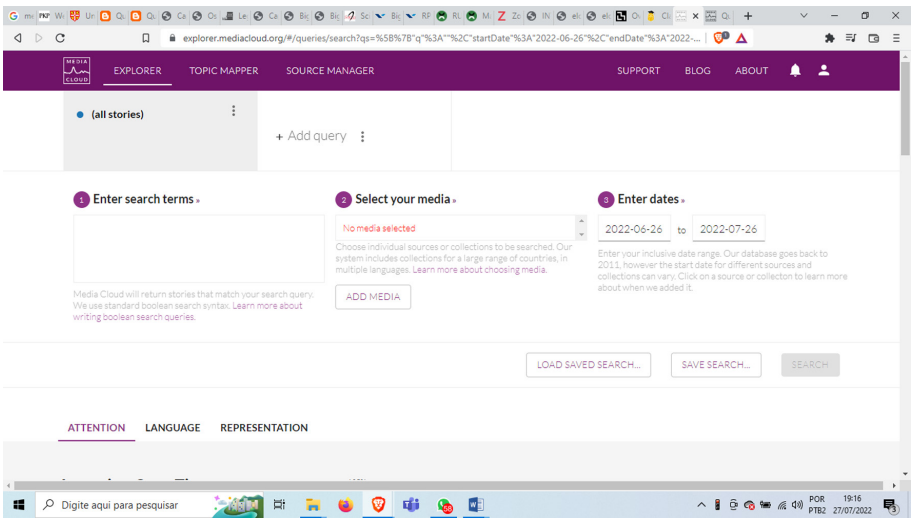

Figura 1 Página inicial do Media Cloud

Fonte: https://explorer.mediacloud.org/#/home.

Com base nas entrevistas realizadas, os termos pesquisados foram: "reconhecimento facial", "OCR", "reconhecimento óptico de caracteres", "drone", "câmera corporal", "câmeras corporais", "*bodycam*", "*bodycams*" e "big data". A fim de delimitar o escopo da busca, os termos obtidos a partir das entrevistas foram combinados com os termos "segurança" (para obter resultados relativos ao termo "segurança pública") e "polícia" ou "policiamento".

Dessa forma, uma vez que a ferramenta *Explorer* utiliza um mecanismo de pesquisa booleana[2], os termos pesquisados foram os seguintes:

1. ("Reconhecimento facial") [and] (policia* or segurança);
2. Reconhecimento [and] (óptico or ótico) [and] caracteres [and] (policia* or segurança);
3. OCR [and] (policia* or segurança);
4. Cameras [and] corporais [and] (policia* or segurança);
5. Camera [and] corporal [and] (policia* or segurança);
6. Bodycam* [and] (policia* or segurança);
7. Drone* [and] (policia* or segurança);
8. ("Big data") [and] (policia* or segurança)
9. ("Policiamento preditivo" or predpol) [and] (policia* or segurança)

A seleção de mídia permite escolher entre fontes específicas ou "coleções", que podem ser agrupadas a partir de diferentes requisitos. Realizamos nossa pesquisa a partir de duas coleções: "*Brazil — National*" e "*Brazil — State & Local*". A primeira das coleções engloba 86 fontes de nível nacional, como os jornais *O Globo*, *Estadão* e *Folha de S.Paulo*, e revistas como *Veja* e *Carta Capital*, além de portais de notícias on-line, como *Uol*, *Bol*, *Yahoo Notícias*. Já a segunda, abarca 1.429 fontes, como jornais, revistas e portais de abrangência estadual, referentes a todos os estados brasileiros.

Quanto ao critério temporal, selecionamos o período de 1º de junho de 2021 a 31 de maio de 2022, correspondente ao período determinado previamente para a realização da primeira etapa de entrevistas e para o mapeamento e monitoramento de notícias relacionadas ao objeto de pesquisa.

Foram obtidos 3.609 resultados, gerados em arquivos .CSV, analisados no programa *Google Sheets*. A limpeza de dados automática, na opção "remover cópias", permitiu a exclusão de 1.197 resultados duplicados. Os 2.412 resultados restantes foram manualmente analisados.

---

2 A pesquisa booleana é um tipo de pesquisa que permite a junção de palavras-chave com operadores (ou modificadores) definidos de maneira específica (como por exemplo, AND, NOT e OR) para produzir resultados de pesquisa direcionados. A explicação sobre o uso de palavras-chave e modificadores pode ser encontrada no seguinte link (em inglês): https://mediacloud.org/support/query-guide.

Em uma primeira etapa de análise das publicações obtidas, resultados que claramente não diziam respeito ao contexto de utilização de tecnologias baseadas em dados por órgãos da segurança pública no Brasil foram descartados.[3]

Posteriormente, os pesquisadores realizaram a leitura de cada um dos resultados restantes, buscando extrair determinadas informações das publicações: o tipo de tecnologia empregada; o âmbito de aplicação — se federal, estadual ou municipal; em se tratando de aplicação estadual, qual o estado; em se tratando de aplicação municipal, qual(is) município(s); o órgão de segurança pública responsável pela utilização da tecnologia — se polícia federal, polícia rodoviária federal, polícia ferroviária federal, polícias civis, polícias militares e corpos de bombeiros militares ou outros órgãos; qual o universo temporal de utilização da tecnologia (se a informação estivesse disponível).

Em relação à estrutura do trabalho, o primeiro capítulo foi dedicado à apresentação do conceito de big data, suas aplicações e funções, correlacionando seu histórico de formação na economia digital e a sua utilização para prevenção e controle de segurança pública — refletindo as características quantitativas do crime, peculiaridades do tempo e do espaço em que ele se insere para execução de práticas consideradas inovadoras para a prevenção de crimes.

O segundo capítulo se debruçou sobre os aspectos normativos da adoção de novas tecnologias e o uso de dados no contexto das investigações criminais, apresentando os desafios para a compatibilização entre riscos e benefícios do uso de tecnologias envolvendo big data na segurança pública e os desafios jurídicos para o processo de regulação do uso dessas ferramentas pelos órgãos de segurança pública e pelo Estado.

O terceiro capítulo contextualizou o leitor acerca das políticas de segurança pública nacionais, suas diretrizes e implementações, apresentando um panorama histórico sobre a utilização da tecnologia na área da segurança pública a nível nacional e, mais detidamente, no município do Rio de Janeiro.

---

3 Exemplos de resultados descartados: "China condena na ONU instrumentalização da ciência pelos EUA na 'reedição da Guerra Fria'". **Hora do Povo**, 24 maio 2022. Disponível em: <https://horadopovo.com.br/china-condena-na-onu-instrumentalizacao-da-ciencia-pelos-eua-na-reedicao-da-guerra-fria/>. Acesso em: 27 jul. 2022."; "Messi no PSG: os bastidores que passam pelos últimos dias no Barça, o choque nos atletas e o fator Neymar para fechar negócio". **ESPN**. Disponível em: <https://www.espn.com.br/futebol/artigo/_/id/9046463/messi-no-psg-os-bastidores-que-passam-pelos-ultimos-dias-no-barcelona-o-choque-nos-atletas-e-o-fator-neymar-para-fechar-negocio>. Acesso em: 27 jul. 2022."; "Usuários têm perfil do Instagram hackeado e golpistas 'vendem' itens". **Gazeta de Vargem Grande**". [s.d.]. Disponível em: <http://www.gazetavg.com.br/2021/12/21/usuarios-tem-perfil-do-instagram-hackeado-e-golpistas-vendem-itens/>. Acesso em: 27 jul. 2022."

No quarto capítulo, foi apresentado o mapeamento dos usos de tecnologia na segurança pública em todo o território brasileiro entre 2021 e 2022. Entre os 27 estados da federação, foram identificados cinco usos mais frequentes de tecnologias: reconhecimento facial, *Optical Character Recognition* (OCR), drones, câmeras corporais (ou *bodycams*) e policiamento preditivo. A tecnologia noticiada como mais utilizada em todo o país foram os drones, com 63% dos estados brasileiros aderentes ao seu uso até o ano de 2022.

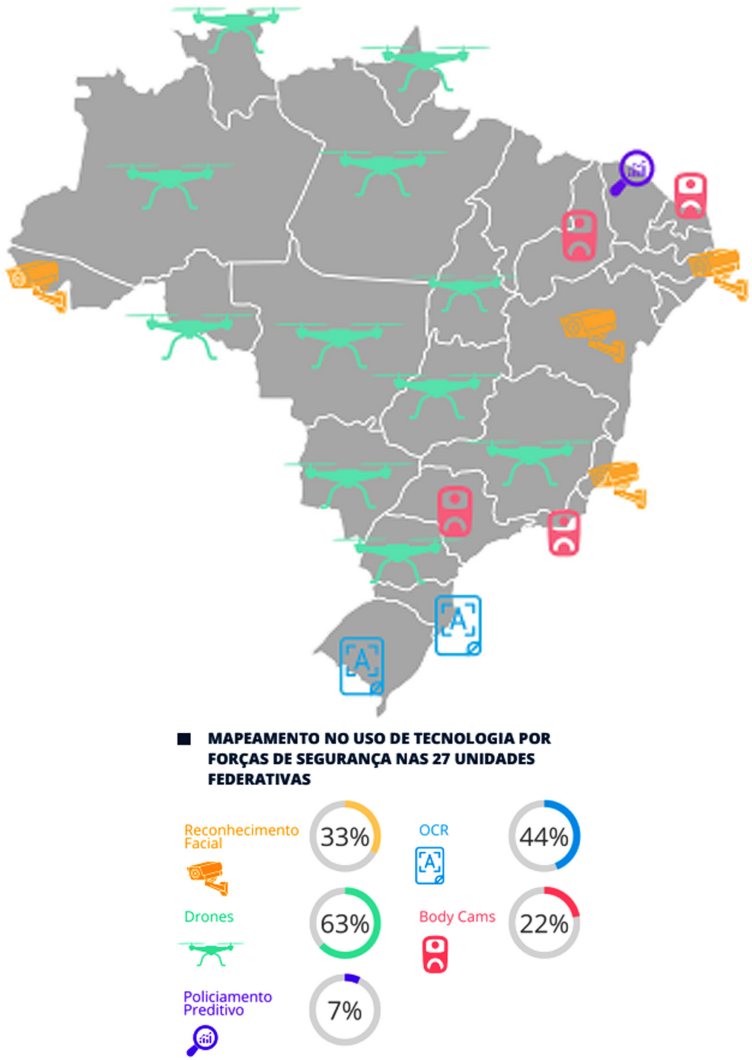

Figura 2 Tipos de tecnologia. Unidades da federação

Por fim, o quinto capítulo foi dedicado às análises das entrevistas realizadas com os agentes de segurança pública, contrastando as mais expressivas consonâncias e dissonâncias dos discursos institucionais às análises documentais do processo de mapeamento, cujas principais fontes de pesquisa repousaram sobre reportagens e publicações de grande circulação sobre o uso de tecnologias baseadas em dados pelas forças de segurança pública no Brasil.

O enfoque deste projeto, e principal farol de investigação, foram as percepções das forças policiais sobre os usos e desusos de tecnologia movida a dados em suas atividades cotidianas. Os dados têm sido um importante ativo na economia digital e uma ferramenta crucial para a solução e coibição de crimes, facilitando o acesso a fichas criminais, boletins de ocorrências e informações sobre focos de criminalidade.

Deste estudo quantitativo e qualitativo se espera oferecer contribuições para os espinhosos debates, estudos e formulações de políticas públicas envolvendo segurança pública e tecnologia em todo o país.

1

Big data e segurança pública

Big data e sociedade da informação

Transformações geopolíticas e econômicas têm modificado o papel da tecnologia no contexto social das últimas décadas. A informação tem sido considerada um ponto central da sociedade contemporânea, que, atravessada por mudanças significativas, levou diversos autores[1] a defenderem a existência de uma nova ordem: a sociedade da informação.

Esse modelo de sociedade se apoia em novos quadros de desenvolvimento econômico, social e cultural decorrentes do processo de globalização, tendo as Tecnologias de Informação e Comunicação (TICs) como definição de um novo paradigma. Dentro dele, indivíduos estariam em um estado contínuo de hiperconectividade, i.e., em absoluta disponibilidade e aptidão para se comunicarem a qualquer momento.

O termo traz alguns desdobramentos, de modo que, além de as pessoas estarem conectadas todo o tempo (*always-on*), também se mostram prontamente acessíveis (*readily accessible*), produzem riqueza de informações e promovem interatividade e armazenamento ininterrupto de dados (*always recording*) (Magrani, 2018, p. 21).

A sociedade da informação se mostra um modelo apoiado no processo de globalização, a "rede global das redes globais" (Castells, 2018, p. 93), que funciona como um espaço de uniformização de conteúdo dentro do qual se articulam as atividades estruturantes das sociedades em termos sociais, econômicos, jurídicos e tecnológicos. A sociedade da informação define as TICs como um novo paradigma para a irrupção de diferentes cenários do que se convencionou denominar desenvolvimento tecnológico.

---

1 Passou a ser utilizado nos últimos anos o termo "sociedade da informação" em substituição à expressão "sociedade pós-industrial", cunhada por Alain Touraine, em 1971, e Daniel Bell, em 1974. Um novo paradigma técnico-econômico emergia, tendo por fator-chave os insumos baratos de informação propiciados pelos avanços tecnológicos na microeletrônica e nas telecomunicações. Essa sociedade pós-industrial, ou informacional, se associa à expansão e reestruturação do capitalismo desde meados da década de 1980, por meio da transformação nos modelos de contrato social entre capital e trabalho, característicos do capitalismo industrial. O desenvolvimento das novas tecnologias e a ênfase na flexibilidade têm fomentado, desde então, rápidas transformações organizacionais. A ver em: BELL, Daniel. **O advento da sociedade pós-industrial**. Tradução: Heloysa de Lima Dantas. São Paulo: Ed. Cultrix, 1974; e TOURAINE, Alain. **The post-industrial society**: tomorrow's social history — classes, conflict and culture in the programmed society. Tradução: Leonard F. X. Mayhew. New York. Random House, 1971. Para mais informações, ver também: CASTELLS, Manuel. **A sociedade em rede**. Volume I. 6. ed. Tradução: Roneide Venancio Majer. São Paulo: Paz e Terra, 2011.

A "tecnologia da informação", segundo Castells, seria definida como o novo grande paradigma moderno no contexto da sociedade da informação. Suas contribuições possuem grande relevância para a compreensão do mundo em termos informacionais e comunicacionais, com perspectiva política, social e econômica, e enfrentam mais um grande desafio no século XXI: a hiperconectividade[2] — termo cunhado pelos cientistas sociais canadenses Anabel Quan-Haase e Barry Wellman em 2005, baseado nas múltiplas possibilidades e usos decorrentes do desenvolvimento das tecnologias de informação e comunicação com a Web 2.0: a mudança para uma internet como plataforma.

A hiperconectividade permite a comunicação através da rede mundial de computadores (*web*) nas modalidades pessoa-a-pessoa, pessoa-máquina e máquina-máquina. Quanto maior o aumento de demanda por conexão de pessoas e dispositivos, maior a complexidade na integração de novos e diversos aplicativos que usam a rede, equipados com recursos de rede com ou sem fio incorporados (Kremer, 2021, p. 27).

No panorama da sociedade hiperconectada, a internet possui um papel fundamental. As pessoas hoje a utilizam como principal forma de comunicação com o mundo e fonte de aquisição de conhecimento. No entanto, essa *web* passa ao largo da premissa utópica que carregava quando de sua criação. O utopismo digital (ou utopismo tecnológico) foi uma ideologia cunhada na década de 1990, no fervor universitário diante do auge da indústria das novas tecnologias no Vale do Silício. Com a premissa de que uma maior conectividade levaria a uma maior coletividade, fundava-se a crença de que a mudança tecnológica revolucionaria os assuntos humanos.

A internet ampliou a capacidade de comunicação como nunca antes, e as pessoas nunca tiveram a possibilidade de estar tão próximas à distância de poucos cliques e toques. Novas formas de comunicação levariam à formação de comunidades e redes sem precedentes em escala pessoal e global (Segal, 2005, p. 151). Para os entusiastas dessa ideologia, a internet seria apenas o precursor das tecnologias digitais que aumentariam a participação democrática, a vida associativa e a liberdade pessoal (Barbrook e Cameron, 2000).

---

2 Hoje, o IPv6 é a tecnologia que dá suporte à ativação de *Internet Protocol* (IP) de todos esses dispositivos e impede explosões massivas de endereços. A ver: QUAN-HAASE, Anabel; WELLMAN, Barry. Hyperconnected network: computer-mediated community in a high-tech organization. In: **The firm as a collaborative community**: reconstructing trust in the knowledge economy. Oxford: Oxford University Press, 2006, p. 281-333.

Era dada a largada para a formação de bancos de dados massivos pelas empresas de tecnologia, a grande matéria-prima do atual monopólio econômico das *Big Techs* — grandes empresas associadas a plataformas de uso intensivo de dados, que se constituem em uma das principais arenas de embates geopolíticos deste século, tendo como ponto nodal o fenômeno do big data. O ato de captar, armazenar e analisar dados não é algo novo na história da humanidade, mas vem se transformando ao longo da trajetória do desenvolvimento tecnológico. O grande crescimento do número de pessoas e dispositivos conectados à rede mundial de computadores, aliado ao exponencial barateamento dos custos para armazenamento de dados, tornam a quantidade de informação gerada e armazenada crescente a cada dia.

Uma pesquisa realizada pela União Internacional de Telecomunicações (agência especializada no tema nas Nações Unidas) identificou que, atualmente, existem 3,2 bilhões de pessoas utilizando a internet em todo o planeta (International Communications Union, 2017), ao passo que quase metade da população mundial têm acesso à conexão (Organização das Nações Unidas, 2016).

Esse cenário está interligado ao big data e já se reflete na realidade empresarial e nos serviços públicos, propiciado sobretudo pelo barateamento de sensores e *hardwares*, das conexões em alta velocidade e do armazenamento e circulação dos dados em nuvem (Gomes, 2019, p. 17).

Não existe uma unanimidade na definição do conceito de big data, mas ele está intimamente ligado à internet das coisas.[3] Este quadro de explosão de informações, lançado pela utilização de tecnologias por pessoas físicas e jurídicas, vem gerando grande interesse de governos e empresas na utilização dos dados gerados e disponíveis para os mais variados fins.

Big data é um termo contemporâneo, surgido no século XXI e inicialmente utilizado por astrônomos e geneticistas, para pensar novas formas e instrumentos de análise para grandes bancos de dados, em função de a memória dos computadores se mostrar insuficiente, até então, para o armazenamento de toda a

---

3 A "internet das coisas" se refere a uma revolução tecnológica que tem como objetivo conectar os itens usados no dia a dia à rede mundial de computadores. Cada vez mais surgem eletrodomésticos, meios de transporte e até mesmo tênis, roupas e maçanetas conectadas à internet e a outros dispositivos, como computadores e smartphones. Cf. ZAMBARDA, Pedro. **Internet das coisas**: entenda o conceito e o que muda com a tecnologia. Techtudo. 16 ago. 2014. Disponível em: <https://www.techtudo.com.br/noticias/noticia/2014/08/internet-das-coisas-entenda-o-conceito-e-o-que-muda-com-tecnologia.html>. Acesso em 05 ago. 2022.

quantidade de informação disponível. Big data é uma expressão bastante ampla, vaga e, por vezes, imprecisa, que comporta diversas interpretações e significados. Especialmente por ser utilizada nos mais diversos campos de conhecimento e setores da sociedade (Gomes, 2019, p. 23-24).

Apesar de ser objeto de ampla difusão e ausente de consenso, algumas definições servem de contribuição e orientação ao presente estudo. Viktor Mayer-Schonberger define big data como coisas realizadas em larga escala que não poderiam ser feitas em escalas menores, para extrair percepções (*insights*) ou criar novas formas de valor de tal maneira, que acabam por modificar mercados, organizações, relações entre cidadãos e governos, entre outros (Mayer-Schonberger, 2013, p. 6).

Dito de outra forma, Schonberger identifica a potência do big data na extração de valor das informações em larga escala. Seu poder e diferencial não se encontram na quantidade massiva de dados em si, mas sim naquilo que pode ser feito a partir da extração dessas informações, ou seja, nas formas de utilização de inteligência sobre os dados, na sua leitura aplicada dentro de um contexto social, seja ele no âmbito privado ou público.

O Grupo de Trabalho do Artigo 29 (GT Art. 29) também conceitua big data de uma maneira bastante interessante, trazendo a visão de que big data se refere a conjuntos de dados gigantescos detidos por empresas, governos e outras organizações de grande porte, que são amplamente analisados usando algoritmos de computador. Ainda para o GT Art. 29, big data pode ser utilizado para identificar tendências gerais e correlações e processado de modo a afetar diretamente os indivíduos.[4]

O termo big data também vem sendo compreendido por alguns especialistas como a expressão de um fenômeno cultural, tecnológico e acadêmico (Boyd e Crawford, 2012, p. 663). Shoshana Zuboff o classifica como o componente fundamental de uma nova lógica de acumulação, com caráter profundamente intencional (Zuboff, 2015, p. 79), não se tratando de um mero objeto, de mera tecnologia ou efeito tecnológico. Para a autora, subdimensionar o conceito de big data desta maneira o reduz à condição de consequência inevitável, fruto de

---

4 O Grupo de Trabalho do Artigo 29 (GT Art. 29) é o grupo de trabalho europeu independente que lidou com as questões relacionadas com a proteção de dados pessoais e da privacidade até 25 de maio de 2018 (data de aplicação do RGPD). Trata-se de uma organização de caráter consultivo e independente, criada pela Diretiva 95/46/ED do parlamento Europeu. Cf. About EDPB: Disponível em: <https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_pt>. Acesso em: 05 ago. 2022.

um "rolo compressor tecnológico" com vida própria e, portanto, supostamente exterior ao que ocorre na sociedade.

Vislumbrar titulares de dados e usuários como meros espectadores não permite que importantes consequências advindas dessa lógica econômica — o que a autora chama de "capitalismo de vigilância" — sejam devidamente escrutinadas. Para ela, trata-se de uma nova forma de capitalismo de informação que busca prever e modificar o comportamento humano como meio de produzir receitas e controle de mercado (Zuboff, 2015, p. 79).

O histórico de formação do big data na economia digital se formou de maneira gradual na última década, incorporando novas políticas e relações sociais que, até então, não haviam sido bem delineadas. Neste aspecto, a autora remonta ao ano de 1997, quando houve um acalorado debate no Federal Trade Comission no qual, enquanto executivos da indústria de tecnologia argumentavam, de um lado, serem capazes de se autorregular e que a intervenção do governo seria tão cara quanto contraproducente, de outro, os libertários civis sustentavam que a capacidade de dados dessas empresas representava uma ameaça à liberdade individual (Zuboff, 2020).

A linha divisória dos limites e possibilidades no uso de dados por essas empresas — hoje gigantes da tecnologia — nunca foi traçada. O capitalismo de vigilância suscitado por Zuboff enraizou-se, floresceu nos novos espaços de internet e culminou em uma lógica econômica dominante, projetada para a ignorância e envolta em desorientação em larga escala.

Zuboff destaca que esses "novos espaços da internet" foram celebrados nos anos 1990 como o maior espaço sem governo do mundo, sem considerar que "o poder preenche um vazio, e aqueles espaços antes selvagens não são mais desgovernados. Em vez disso, eles pertencem e são operados pelo capital de vigilância privado e governados por suas leis de ferro" (Zuboff, 2020, p. 4).

O presente estudo não possui a pretensão de esgotar o tema, ou oferecer uma definição final sobre o disputado conceito de big data. No entanto, após uma leitura detida sobre suas aplicações e funções nos mais diversos campos de conhecimento, dentro e fora do direito, entende-se por big data a análise de grandes quantidades de dados, realizada de maneira automatizada por algoritmos, com intuito de extrair resultados e benefícios (Gomes, 2019, p. 29). Isso vislumbrando-se ainda que big data é menos sobre dados e mais sobre a capacidade de pesquisa, agregação e referência cruzada de grandes conjuntos de dados (Boyd e Crawford, 2012).

Big data como ferramenta no combate à criminalidade

O big data também tem sido utilizado no campo da prevenção e controle na segurança pública, situação em que é mobilizado para refletir de forma abrangente as características quantitativas do crime, peculiaridades do tempo e do espaço em que ele se insere, além de eventuais processos de mudança observáveis dentro de um período. Alguns autores têm denominado esse campo de atuação como big data criminal, cujo valor se reflete principalmente em práticas consideradas inovadoras para a prevenção de crimes (Cai, Li e Wang, 2020, p. 2).

No cenário internacional, alguns departamentos de polícia dos Estados Unidos, como a polícia de Santa Cruz, no estado da Califórnia, têm utilizado big data para analisar casos históricos anteriores de crimes cometidos, encontrando assim tendências e padrões que se repetiam com o decurso do tempo. Outros estados da federação, como Maryland, utilizam tecnologias preditivas para levantamento das possibilidades de reincidência de infratores ou revisão de liberdade condicional, aplicadas pelos sistemas de justiça.

Outro exemplo, também nos Estados Unidos, é o da polícia da Carolina do Sul, que utilizou ferramentas de análises de dados da IBM para explorar padrões de crimes, identificar pontos críticos, buscando otimizar a atuação da polícia. Já o departamento da polícia de Los Angeles fez parcerias com instituições de pesquisa para desenvolver sistemas e softwares capazes de prever locais de alto risco para cometimento de crimes.

Na China, o quadro não tem sido diferente. A análise criminal com big data, denominada "policiamento da informação", vem se solidificando como um importante suporte na região para a prevenção e o controle social na segurança pública. A exemplo do Departamento de Segurança Pública da polícia de Shandong, no qual a construção da plataforma em nuvem da organização viabilizou a coleta de 36,9 bilhões de dados em 2016, e o volume total de armazenamento atingiu dez petabytes de informação (Cai, Li e Wang, 2020, p. 3).

Ainda em 2013 foi iniciada uma cooperação entre a Secretaria Municipal de Segurança Pública de Pequim, na filial de Huairou, e a Universidade de Tecnologia de Tianjin. O objetivo era o desenvolvimento de um sistema de análise de dados criminais e previsão de tendências, cujas aplicações práticas, bastante substanciais, desdobram efeitos até os dias atuais (Chen T *et al*, 2014, p. 10).

Esses exemplos têm por objetivo demonstrar que Estados Unidos e China, os países que atualmente despontam na corrida internacional pela dianteira no desenvolvimento da inteligência artificial, têm aplicado vigorosos investimentos em tecnologia no campo da segurança pública na última década. Mas essas aplicações não se dão à margem de um intenso debate social a respeito do papel que tais tecnologias detêm nesse cenário, ou de potenciais riscos em relação aos direitos fundamentais e interesses coletivos. Pelo contrário, uma série de iniciativas têm ganhado corpo desde 2020 nos próprios estados da federação no território estadunidense, algumas até mesmo em prol do banimento de tecnologias, na contramão até mesmo de iniciativas anteriormente já implementadas.[5]

No Brasil, autores como Mauricio Dieter têm denominado este fenômeno como "política criminal atuarial", entendendo por atuarialismo a aplicação de critérios de prognose para determinar uma tomada de decisão (Dieter, 2021, p. 85). Para o autor, a política criminal atuarial se desenvolve dentre três tendências da política criminal contemporânea: o populismo, o internacionalismo e o gerencialismo. Essas três perspectivas não conflitam, ao contrário, convergem na medida em que reestruturam o discurso punitivo, tendo na política criminal atuarial uma forma de distribuição de justiça conforme o grupo de risco ao qual a pessoa pertence.

Dieter afirma que a ideia de uma justiça atuarial no sistema de justiça criminal implica em utilizar prognósticos acumulados, e o longo acúmulo de dados constituirá um repertório de big data a partir do prognóstico de reincidência que uma pessoa tem no sistema criminal (Dieter, 2021, p. 86). Desse modo, a característica geral desses mecanismos prognósticos seria a definição do risco pelo comportamento e situação de vida marginal.

Dito de outra forma, o autor entende que os sistemas que usam prognósticos de risco seriam caros e ineficientes, o que coincidiria com o giro punitivo, cuja maior expressão é o encarceramento em massa. Em termos de prevenção,

---

5 Santa Cruz estava entre as primeiras cidades dos EUA a adotar o policiamento preditivo em 2012, mas em 2020 a cidade da Califórnia se tornou a primeira do país a proibir a política. Em decisão unânime na Câmara Municipal, aprovou-se uma portaria que proibia o uso de dados para prever onde os crimes poderiam ocorrer, e também proibiu a cidade de usar software de reconhecimento facial. Cf. STURGILL, Kristi. Santa Cruz becomes the first U.S. city to ban predictive policing. Tradução nossa. 2020. **Los Angeles Times**. 26 jun. 2020. Disponível em: <https://www.latimes.com/california/story/2020-06-26/santa-cruz-becomes-first-u-s-city-to-ban-predictive-policing>. Acesso em: 05 ago. 2022.

a política criminal atuarial traria questões sociais graves no chamado efeito cremalheira,[6] desenvolvido por Bernard Harcourt, trazendo um custo social (Dieter, 2012, p. 233). Harcourt, portanto, negará que a concentração da repressão em desfavor de grupos sociais estatisticamente vinculados à prática de certos crimes resultará em necessária diminuição dos índices de criminalidade, seja no interior do próprio grupo de risco, seja em relação ao total da população (Harcourt, 2007, p. 34-35).

Não há respostas fáceis para a combinação entre big data e as necessidades atuais de prevenção ao crime e ao controle, sobretudo considerando os tensionamentos entre estigmatização e controle social. Os dados na investigação criminal exigem dupla atenção pois, de um lado, são o meio a partir do qual boa parte da inteligência investigativa será direcionada. De outro, os próprios dados podem se tornar alvo de ataques criminosos, ou mesmo de usos enviesados a partir da operação de dados e das informações por ela geradas. É importante reconhecer que a enorme quantidade de informações contidas em grandes bancos de dados pode ser alvo e instrumento de abuso, dentro do processo de coleta e utilização, de modo a levar a sério os desafios da aplicação de big data para prevenção e controle na seara criminal.

Novas tecnologias e os novos desafios para a segurança pública

O paradigma do big data está presente em todos os aspectos da investigação criminal. Computadores pessoais e laptops tiveram um crescimento constante no que diz respeito ao armazenamento, tornando-se comum a existência de disco rígido com terabytes de espaço. Além disso, a popularidade dos telefones celulares aumentou. Estes, que foram transformados de simples terminais de comunicação de usuário final em uma ferramenta poderosa e engenhosa capaz de computação paralela. Eles também estão armazenando uma variedade de dados de log de várias fontes, como Sistema de Posicionamento Global (GPS) e outros sensores, além de fotos, músicas e documentos do usuário.

Como resultado, eles podem armazenar centenas de gigabytes de dados pessoais e informação sensível. Há uma forte necessidade de dados avançados

---

6 Efeito cremalheira é uma tradução livre utilizada por Mauricio Dieter para se referir ao "ratchet effect", de Bernard Harcourt. No intuito de traduzir a ideia de um mecanismo que, uma vez acionado, não permite o retorno à situação anterior. Assim como a cremalheira dos lacres de plástico ou as chaves roquete aplicadas a uma porca. Cf. HARCOURT, Bernard E. **Against Prediction: profiling, policing and punishing in an Actuarial Age**. Chicago (Illinois): The University of Chicago Press, 2007.

e análises para ajudar nas investigações, o que requer novas abordagens para uma gestão mais eficiente e eficaz.

As reformas tecnosolucionistas impulsionadas pelos avanços das tecnologias de informação e comunicação, sobretudo aquelas referentes ao big data e à inteligência artificial, estão reconfigurando as normas, práticas e relações sociais no policiamento e na segurança pública em todo o mundo. O aceleramento das mudanças de diferentes tipos de tecnologia tem alterado fundamentalmente o panorama da segurança pública: avanços tecnológicos profundos nas áreas da computação e da ciência de dados, pareados com a mudança global para comunicações e transações em rede digital, transformaram o cenário político e econômico a um nível global — o que, como veremos, inclui o caso brasileiro.

Fato é que a tecnologia sempre teve um papel decisivo na construção das relações sociais e das políticas relacionadas à segurança. O desenvolvimento e a introdução de tecnologias de guerra, como armas de pequeno porte, bombas nucleares ou mísseis teleguiados, alteraram a questão de segurança a nível global e, em alguns casos, afetaram as relações internacionais; ao passo que tecnologias civis mais "prosaicas", como a internet e as redes sociais, também trouxeram consequências significativas para as políticas de segurança. Em cada um desses casos, os formuladores de políticas de segurança nacional tiveram que fazer um balanço de sua abordagem, reexaminar as teorias e práticas de guerra existentes e determinar como as organizações e estratégias deveriam se adaptar à luz de novas ferramentas.

Nos últimos anos, o desenvolvimento tecnológico girou em torno de tecnologias baseadas em dados. Exemplos não nos faltam: avanços recentes na área de Inteligência Artificial (IA), por exemplo, especificamente no campo da IA conhecida como aprendizado de máquina (*machine learning*, em inglês), têm permitido que computadores interpretem e "compreendam" atividades antes restritas ao domínio humano, como controlar veículos, jogar jogos de tabuleiro, tomar decisões das mais variadas ordens, reconhecer pessoas e até mesmo julgá-las criminalmente.

Além da IA, diversas outras tecnologias se desenvolveram, como *blockchain*, criptomoedas, computação quântica e redes de banda larga de quinta geração (conhecidas popularmente como "5G") — que, por sua vez, supostamente

permitirão o pleno desenvolvimento da chamada "internet das coisas" (*IoT,* no acrônimo em inglês), objetos cotidianos plenamente conectados à internet.

Com o avanço do mecanismo estratégico de análise de dados, o big data passa a integrar o arsenal de ferramentas de combate à criminalidade, através da aplicação de tecnologias de tratamento de dados à atividade policial e à persecução penal. Esse processo, apesar de gradual, já vem produzindo impactos concretos, como demonstrado na cidade de Chicago, nos Estados Unidos. Segundo relatório de Chicago Tonight, não só na cidade como um todo a criminalidade reduziu em 13%, como nos dois distritos onde a tecnologia do big data foi introduzida, houve uma redução de 49% e 66% no número de tiroteios nos meses de fevereiro e março de 2017 (Saisse, 2017, p. 5).

A obtenção e armazenamento de dados promete otimizar a segurança pública, além de baratear os custos operacionais. Para mais, o uso de reconhecimento facial, tal como o acesso aos dados coletados, como ficha criminal e outras informações de possíveis suspeitos, facilita o trabalho da polícia, possibilitando a realização de diligências preventivas na identificação da criminalidade.

Além disso, as técnicas do big data possibilitam o mapeamento de índices de criminalidade e permitem acesso à base de dados de diferentes órgãos públicos, ampliando ainda mais as informações disponíveis. Ainda que represente um grande avanço, o uso de inteligência artificial pode causar certo estranhamento, isso porque os agentes entram em contato com uma nova tecnologia, necessitando de um treinamento para que possam usufruir dos benefícios trazidos por ela.

O ingresso do big data no Brasil contou com quatro programas: Sinesp Big Data, o Sinesp Geo Inteligência, o Sinesp Tempo Real e o Sinesp Busca, introduzidos por meio do "Em Frente Brasil", projeto piloto elaborado para o combate à criminalidade, no Espírito Santo, em Goiás, no Pará, no Paraná e em Pernambuco.

Tendo em mente que o uso de dados é controverso, a partir do momento que pode, facilmente, ser manipulado, segundo o diretor de Gestão e Integração de Informações da Secretaria Nacional de Segurança Pública, Wellington Porcino, todos os municípios devem contar com gestores de estatística e de tecnologia da informação para garantir a eficácia e a qualidade dos dados.

Como vimos, a tecnologia do big data possibilita a facilitação do acesso aos dados, bem como a integração de bases de dados de todo o Brasil, de maneira que a força policial e os agentes de segurança têm a possibilidade

de utilizar esses dados na análise da atividade criminal, acessando as fichas com mais facilidade, além de boletins de ocorrências e informações sobre focos de criminalidade. Dessa forma, através do compartilhamento de informações entre estados da federação, as fronteiras deixam de ser um limitador tão grande, possibilitando um combate à criminalidade difundido ao longo do território nacional.

2

Aspectos normativos da adoção de novas tecnologias pela segurança pública

Uso de dados no contexto da segurança pública

O fenômeno do big data tem desafiado a sociedade e o ordenamento jurídico diante da grande quantidade de informações pessoais coletadas, armazenadas e analisadas. Como vimos, o tratamento de grandes volumes de dados na sociedade hiperconectada não apenas viabiliza que corporações e governos possam tratar enormes quantidades de informação, propondo benefícios e otimização de serviços em prol de avanços sociais, como também expõe a riscos os usuários e a própria sociedade, devido a potenciais violações de direitos que sobrevêm às tecnologias (Gomes, 2019, p. 42).

A compatibilização entre riscos e benefícios do uso de tecnologias tem sido o ponto central dos debates envolvendo big data e segurança pública. De tal modo que o direito tem sido trazido como ferramenta de embate das injustiças e importante instrumento de coibição de abusos e riscos que o uso de novas tecnologias pelos órgãos de segurança pública e pelo Estado possam infringir aos indivíduos e à sociedade como um todo.

A proteção de dados pessoais tem se tornado discussão fundamental nos últimos anos, à medida que avança a constante coleta de dados pessoais, gerada pelo uso massivo de serviços e de bens conectados à internet, associada ao contínuo monitoramento que é feito dos hábitos e comportamentos das pessoas dentro e fora da rede (Mulholland e Frajhof, 2020, p. 11).

No Brasil, a Lei Geral de Proteção de Dados (LGPD) entrou em vigor em 18 de setembro de 2020, após longas e tortuosas articulações entre Congresso Nacional e o Governo, com o envolvimento de diversos atores e setores da sociedade. Suas sanções (multas e penalidades por descumprimento), por sua vez, passaram a ser aplicadas em agosto de 2021. No entanto, o texto legal exclui do âmbito de sua aplicação os casos de tratamento de informações para fins de segurança pública e persecução penal.

Apesar de a LGPD não regular diretamente os casos de uso de dados nessas condições, alguns pontos interessantes merecem ser considerados. O primeiro é que a LGPD garante a edição de uma lei específica para questões relativas ao uso de dados pessoais pelos órgãos e agentes de segurança pública, norma que garantirá o devido processo legal, os princípios de proteção de dados e os direitos dos titulares (Costa e Reis, 2021). Em 2019, a Câmara dos Deputados tomou a iniciativa de criar uma comissão de juristas para a elaboração de um anteprojeto de lei da chamada LGPD Penal, formada por quinze membros estudiosos da

intersecção entre proteção de dados e segurança pública, dentre os quais Laura Schertel (relatora), Danilo Doneda, Tércio Sampaio Ferraz Jr. e outros.

Para subsidiar as discussões, foi organizado um seminário internacional cujos painéis abordaram temas relevantes e espinhosos para o campo, dentre os quais: banco de dados de DNA, reconhecimento facial e transferência internacional de dados. Como resultados obtidos, levantou-se o interesse comum de construção de uma lei que não inviabilize o tratamento de dados nas atividades policiais, mas que garanta direitos fundamentais e crie situação de confiança entre o Estado e o cidadão (Costa e Reis, 2021).

O anteprojeto já foi finalizado e atualmente se encontra na Câmara dos Deputados, à espera de um parlamentar que o apresente formalmente para que se torne um Projeto de Lei (PL) e siga os trâmites comuns do processo legislativo: avaliação pelas comissões, voto, envio ao Senado e submissão à sanção presidencial. Também se encontra em trâmite no Congresso Nacional uma segunda proposta legislativa de LGPD Penal: o PL 1.515/22, de autoria do então deputado Coronel Armando, que não obteve reeleição em 2023. O PL tem sido alvo de críticas por parte da sociedade civil pelos direitos digitais no Brasil que, após análises comparativas e apontamentos críticos sobre seus arranjos normativos, recomenda o seu arquivamento devido à supressão de diversas garantias dos titulares e ampliação excessiva do poder discricionário do Estado (Azevedo *et al*, 2022).

O segundo ponto relevante é que a LGPD, apesar de não tratar diretamente sobre proteção de dados e segurança pública por vedação expressa no seu Art. 4º, apresenta alguns parâmetros e garantias que devem ser observados ao longo do seu texto. E não apenas por isso, o período compreendido entre 2020 e 2022 foi marcado por algumas decisões muito relevantes no Supremo Tribunal Federal no que diz respeito ao direito à proteção da privacidade e dos dados pessoais.

Em 2020, o Supremo Tribunal Federal (STF) deu um importante passo ao reconhecer um direito fundamental autônomo à proteção de dados pessoais, no julgamento das Ações Diretas de Inconstitucionalidade (ADIs) 6.387, 6.388, 6.389, 6.393 e 6.390. Com a promulgação da Emenda Constitucional (EC) 115, em fevereiro de 2022, a proteção de dados pessoais tornou-se expressa na Constituição Federal e foi elevada à categoria de direito fundamental, acrescendo-se ao Art. 5º o inciso LXXIX. Isso produz efeitos muito relevantes para fins de proteção de direitos no campo da segurança pública, a despeito da existente lacuna legal explícita sobre o tema.

Pouco tempo depois, em setembro de 2022, o STF teve a oportunidade de julgar a ADI 6.649, proposta pelo Conselho Federal da Ordem dos Advogados do Brasil (OAB Federal), que questionava a constitucionalidade da estrutura de compartilhamento de dados da Administração Pública Federal, amparada pelo Decreto 10.046/19, que cria o Cadastro-Base do Cidadão. Uma base integrada que contém dados gerais sobre todos os brasileiros, acessível a todos os órgãos do Executivo Federal mediante adesão. O decreto estabelece como finalidades do compartilhamento de dados a simplificação de serviços públicos, a redução de custos com o reaproveitamento de sistemas de informática e também a análise do direito a benefícios sociais. Um importante teste para este novo direito fundamental e uma oportunidade para a consolidação das balizas constitucionais do tratamento de dados pessoais no Poder Público.[7]

No julgamento, o STF acabou por não apenas validar a constitucionalidade do decreto atacado pela OAB Federal, no sentido da possibilidade do compartilhamento de informações, como também condicionou a permissão de acesso aos dados a parâmetros demasiado abertos, tais como: propósitos legítimos, específicos e explícitos, e atendimento do interesse público. Um cadastro complexo e demasiado robusto, que comporá seu banco também com dados biométricos (portanto sensíveis) da população brasileira, sem garantias adicionais a esse tratamento e sem a presença de qualquer tipo de instrumento de prestação de contas apto a indicar as finalidades no âmbito da administração pública, entre outros diversos flagrantes vícios de constitucionalidade.

A decisão do STF se mostra conflitante com a construção jurisprudencial que se vinha tecendo, que correlacionava proteção de dados pessoais e exercício pleno da democracia. Frise-se que, à ocasião do julgamento do caso paradigmático sobre o Censo Demográfico na Alemanha em 1983, a Corte Constitucional afirmou a importância de cidadãos serem capazes de saber quem sabe o que sobre eles, quando e em que situação, para que não lhes sobrevenham prejuízos no desenvolvimento de sua personalidade, para sua autodeterminação informativa e para o bem comum de uma sociedade democrática.[8]

---

7 MENDES, Laura Schertel. Democracia, poder informacional e vigilância. Fumus Boni Iuris. **O Globo**. 13 ago. 2022. Disponível em: <https://oglobo.globo.com/blogs/fumus-boni-iuris/post/2022/08/laura-schertel-democracia-poder-informacional-e-vigilancia.ghtml>. Acesso em: 20 out. 2022.

8 BVerfGE [Decisões do Tribunal Constitucional Federal] 65, I — decisão sobre o censo populacional.

O campo jurídico-penal é alvo de disputas constantes, no sentido das reiteradas denúncias de seletividade penal feitas em face dos órgãos do sistema de justiça e do sistema criminal, quanto à construção do status de criminoso na sociedade e da funcionalidade do sistema jurídico-penal para a manutenção das desigualdades e reprodução de hierarquias de poder. A proteção de dados, assim como o direito penal, não tem seus debates jurídicos eivados de intencionalidade ou tensionamentos políticos, apesar de a cultura de proteção de dados no Brasil ainda ser jovem e estar em franca expansão.

A incorporação de ferramentas tecnológicas pelas forças de segurança torna esse cenário ainda mais complexo. O objetivo de atribuir maior eficiência à atuação policial traz consigo uma problemática, que reside na adoção às cegas dessas mesmas ferramentas. Têm sido adotadas tecnologias que não são neutras em seus usos e em seu desenvolvimento, razão pela qual é importante uma reflexão sobre a importância da regulação dessas tecnologias e os riscos de reprodução de padrões historicamente estabelecidos e consolidados no seio social, reforçados pelo uso de novos aparatos tecnológicos (Arruda *et al*, 2021, p. 666).

Inteligência artificial e investigações criminais

Nos idos de 1950, algumas das mentes pioneiras no campo até então emergente da ciência da computação (Marvin Minsky, John McCarthy e Herbert Simon) estabeleceram como missão recriar a inteligência humana na máquina, ou ao menos aquilo que se entendia por inteligente, ao que se convencionou nomear este novo ramo de Inteligência Artificial (IA). Hoje, o termo apresenta atecnias de tal modo que sua própria etimologia não reflete mais os novos contornos adquiridos por essa tecnologia. Isto porque reduzir as funções e possibilidades da IA à mera replicação da inteligência humana por máquinas implicaria em diminuir demasiadamente as suas capacidades e potencialidades, e o big data possui um papel central nesse processo.

Não existe consenso na literatura científica em relação ao conceito de IA, mas suas definições costumam ser categorizadas empiricamente e teoricamente. O que significa dizer que, na ótica da categoria empírica, existe a perspectiva de os sistemas pensarem como seres humanos e aprenderem a partir da experiência. Ou seja, a partir do uso da tecnologia ocorreriam formulações de hipóteses e confirmações experimentais. Enquanto isso, no enfoque teórico esperam-se ações lógicas, que incluem capacidade de dedução e inferência sobre novas

relações (Alves, 2020). O reconhecimento de padrões e aplicação de regras lógicas são elementos relevantes no modo de funcionamento das técnicas de IA.

Independente da categoria adotada para definir inteligência artificial, o que torna possível seu aprendizado com dados e aprimoramento de novos conjuntos de regras e métodos são os algoritmos: conjuntos de instruções não dúbias que um computador pode executar. São os algoritmos de aprendizado que podem conduzir à descoberta e à resolução de problemas por meio de estratégias e inferências (Alves, 2020). As aplicações de IA apenas são possíveis para a solução de problemas da área da ciência da computação a partir da disponibilidade abundante de dois insumos fundamentais: bancos de dados massivos e grande poder computacional.

Em sua última chamada de trabalhos, a Association for the Advancement of Artificial Intelligence (AAAI) considerou *machine learning* (ML) e big data uma das nove subáreas que compõem as aplicações de IA.[9] Além disso, um ramo de ML que tem se destacado é o Deep Learning, com métodos dinâmicos que prometem capacidade contínua de melhora e adaptação a mudanças de padrões e a concretização de sistemas preditivos. Este ramo detém capacidade de reconhecimento de padrões complexos e numerosos e com função de aprendizado, tendo como um de seus métodos as Redes Neurais Artificiais (RNA), baseadas na arquitetura dos neurônios humanos e destinadas a reproduzir aprendizado por meio do desenvolvimento de sistemas que aprendem com exemplos de treinamento.

No campo da segurança pública, as RNA são técnicas da IA aplicadas para fins de policiamento preditivo: sistemas computadorizados cujo processamento de informações por algoritmos se utilizam tanto de bancos de dados robustos quanto de análises estatísticas para fins de predição de um acontecimento criminoso futuro (Moraes, 2022, p. 35).

O policiamento preditivo associa técnicas computacionais sofisticadas, bancos de dados massivos (big data) e a estatística e oferece muitas promessas para a adoção de estratégias policiais mais efetivas à segurança pública. É o caso da predição de crimes, de ações para redução da criminalidade e até mesmo do

---

9 A Association for the Advancement of Artificial Intelligence (AAAI) é considerada uma associação de referência e na sua última chamada de trabalhos dividiu as aplicações em nove subáreas: Pesquisa; Machine Learning, Data Mining e Big Data; Planejamento Automatizado; Representação de Conhecimento; Raciocínio (Probabilístico ou não); Processamento de Linguagem Natural; Robótica; Sistema de Agente e Multiagente e Aplicações. Cf. https://www.aaai.org/home.html.

perfil de sujeito que pode vir a cometer um delito. Trata-se de um desejo antigo de gestores públicos e forças policiais que começou a ganhar atenção no início dos anos 2010, quando algumas cidades nos Estados Unidos passaram a testar e utilizar esse tipo de ferramenta no trabalho policial.

Durante esse período, companhias como PredPol e Palantir passaram a vender soluções tecnológicas em Chicago, Nova Iorque e Nova Orleans. Em 2021, foi veiculada a compra de tecnologias dessa natureza em cidades brasileiras. No caso do Rio de Janeiro, uma investigação do jornal *The Intercept Brasil* identificou a compra de um enorme pacote de serviços de infraestrutura da multinacional Oracle, com softwares capazes de fazer cruzamentos e análises de grandes volumes de dados. A tecnologia oferecida às autoridades policiais permitiria reunir diferentes bases de dados, organizar e hierarquizar informações como: ocorrências policiais, armas de fogo, celulares, veículos, pessoas e até mesmo dados biométricos, facilitando o acesso aos policiais e otimizando recursos (Dias e Hvistendahl, 2021).

As RNAs, portanto, têm se mostrado um recurso importante para o desenvolvimento de novas tecnologias que estejam à altura dos novos desafios enfrentados no campo da segurança pública. As tecnologias de inteligência artificial, como visto, não são tão inteligentes assim. Elas aprendem a partir do reconhecimento de padrões, de modo que as características do que se pretende ensinar a uma RNA irão definir o modelo de arquitetura utilizada, ou seja, dependendo do que a tecnologia de IA vai precisar aprender. Dentre as dez principais arquiteturas de RNA (Goodfellow, 2016), destacam-se três no campo da segurança pública atualmente: as Redes Multilayer Perceptron (MLP), as Redes Neurais Convolucionais (RNC) e as Redes Neurais Recorrentes (RNR).

O MLP é utilizado em casos de aprendizado supervisionado, ou seja, a máquina é treinada usando dados denominados "rotulados" (já conhecidos, não inéditos para ele). Esses dados foram previamente identificados com rótulos que identificam alguma característica, servindo de base para os algoritmos promoverem tomadas de decisão a partir das informações disponíveis. Resolvendo problemas conhecidos e usando um conjunto de dados rotulado para treinar um algoritmo a realizar tarefas específicas como reconhecimento e classificação de padrões em imagens e arquivos de áudio, por exemplo.

As RNR são eficientes para aprendizado com dados sequenciais, dados temporais e processamento de linguagem natural, comumente aplicadas para

modelagem de linguagem e reconhecimento de fala (Graves e Abdel-Rahman, 2013). Ao passo que as RNC se destacam na classificação de imagens e agrupamento por similaridades, a exemplo do Reconhecimento Óptico de Caracteres (OCR), tecnologia que vem sendo amplamente utilizada pelas secretarias de segurança pública dos estados, instaladas em câmeras de videomonitoramento para leitura de placas de veículos e motocicletas.

O big data tem se mostrado uma janela de oportunidades para a solução de alguns dos principais desafios que se arrastam no campo da segurança pública, conferindo centralidade às realidades enfrentadas por cada força policial em termos de demanda, regionalidade e integração informacional. No entanto, não sem riscos. A inteligência artificial é uma tecnologia de propósito geral e de aplicações diversas, que carece de parâmetros de segurança determinados pelo Estado, na construção de uma relação de comando e controle.

O cenário jurídico brasileiro atual, que já carece de uma legislação de proteção de dados pessoais aplicada ao contexto da segurança pública e persecução penal, ganha contornos ainda mais dramáticos no contexto da IA. Apesar dos inegáveis benefícios, tais aplicações trazem casos correntes de vieses de gênero, raça, classe, sexualidade e são capazes de potencializar os efeitos perigosos e pervasivos da vigilância excessiva e do tecnoautoritarismo por parte dos agentes estatais.

No ano de 2023, o Senado Federal caminha em direção a um novo cenário regulatório envolvendo a IA no Brasil, espalhando seus efeitos no campo das investigações criminais. Em dezembro de 2022, foi elaborada uma ementa de substitutivo aos Projetos de Lei 5.051/19, 21/2020 e 872/2021 pela Comissão de Juristas responsável por subsidiar a elaboração de substitutivo sobre Inteligência Artificial no Brasil (CJUSBIA), trazendo novos dispositivos. A minuta do anteprojeto de lei denominado “Marco legal da Inteligência Artificial no Brasil” já foi entregue ao presidente do Senado em dezembro de 2022, após oito meses de intenso trabalho e oitiva da comunidade brasileira e internacional em caráter multissetorial.

Tem-se um cenário regulatório complexo, à altura dos desafios que se lhe impõem as discussões e sopesamentos entre o aparelhamento tecnológico dos órgãos de segurança pública e a proteção de direitos fundamentais.

De um lado, a necessária regulação de uma tecnologia que já vem sendo amplamente adotada pelos setores público e privado e que já encontra substanciais

aportes econômicos por parte da União, estados e municípios no processo de aquisição e implementação dos mais diversos aparatos contendo sistemas de IA. Do outro, a mitigação de violências e vieses discriminatórios potencializados por maus usos de tecnologias de IA, impactando a proteção de bens jurídicos tutelados, como privacidade, dignidade humana, acesso a oportunidades e serviços públicos essenciais, livre circulação e até mesmo o reforço de estereótipos discriminatórios, sobretudo raciais.

A aplicação de sistemas de IA com aprendizado de máquina traz consigo grandes promessas para a solução de algumas das principais mazelas sociais, como o combate à violência, à letalidade e a garantia da segurança. No entanto, é essencial que o uso de quaisquer tecnologias na segurança pública e na esfera de persecução penal não sejam mais um fator de violação de direitos, razão pela qual a regulação se mostra tão importante para fins de segurança jurídica, garantia dos direitos fundamentais, gradação de riscos e responsabilização pelo uso da tecnologia de IA e seus impactos para a sociedade.

Provas digitais na legislação penal e processual penal

Nos últimos dois anos de entrada em vigor da LGPD, as provas digitais têm tido relevância nos debates públicos. Apesar dos avanços na promoção de garantias de direitos fundamentais no contexto do uso da internet e de novas tecnologias com os marcos normativos da LGPD e do Marco Civil da Internet (MCI), ainda não é possível aferir uma moldura normativa para a sedimentação de processos protetivos e garantia de segurança jurídica no contexto das investigações criminais.

O horizonte jurídico brasileiro ainda carece de maior delineamento na aferição dos mecanismos de proporcionalidade para uso de novas tecnologias na produção de provas, a fim de evitar vigilância excessiva, arbitrariedades e eventuais prejuízos à eficácia da ação penal como um todo. Duas articulações legislativas ocorridas em 2021 foram muito importantes para o contexto de regulação da produção de provas digitais no âmbito penal: a reforma do Código de Processo Penal (CPP) e o anteprojeto da LGPD Penal.

A tramitação do texto do Projeto de Lei n. 8.045/2010, do Senado Federal, trata das propostas de alteração ao Código de Processo Penal (CPP). Dentre as matérias abordadas no PL, chama a atenção o capítulo relativo às provas digitais. A forma como temas de tecnologia e uso de dados foram abordados na redação do texto tem sido alvo de atenção de acadêmicos e ativistas, na medida

em que pode expandir, legitimar e institucionalizar a vigilância estatal sobre as comunicações no Brasil de forma alarmante.

A despeito de se mostrar urgente a atualização do processo penal brasileiro para a era digital, ativistas e estudiosos atentam desde 2021 para os riscos de se atingirem garantias constitucionais e o devido processo legal com as alterações em curso, as quais precisam estar na base do Estado Democrático de Direito. Dentre algumas das principais críticas promovidas pela Coalizão Direitos na Rede (CDR), que reúne cerca de sessenta organizações acadêmicas e da sociedade civil que atuam em defesa dos direitos digitais no Brasil (Coalizão, 2021), destacam-se: (i) expansão desproporcional da retenção massiva de dados para futuras investigações; (ii) retrocesso em garantias no âmbito da interceptação de comunicações; (iii) criação de exigências aos provedores que podem significar a introdução de vulnerabilidades de segurança em seus sistemas e serviços e (iv) legitimação de *hacking* governamental, isto é, quando os investigadores do governam usam vulnerabilidades (*bugs*) em sistemas e máquinas para obter acesso remoto a computadores, interferir em seu funcionamento e/ou monitorar atividades do usuário.

A proposta do novo CPP, em especial no tocante às provas digitais, apresenta alguns retrocessos a partir de definições imprecisas e desequilíbrios na tutela jurídica da prova digital. A abertura de brechas para situações abusivas no curso de investigações e processos pode levar a cenários de abusos e criar capacidades demasiado intrusivas, potencializando estigmas sociais e discriminações já presentes no tecido social brasileiro, reforçadas pelas atuações das forças de segurança. Razão pela qual essas hipóteses de meios de provas estão em disputa pela sua exclusão no texto final do PL.

Setores do Ministério Público e polícia federal, por sua vez, têm demandado em suas rotinas investigativas a inserção de novos mecanismos de vigilância, interceptação e extração de dados. Com essa movimentação política, a sociedade civil tem pleiteado por instrumentos protetivos capazes de oferecer a cobertura necessária aos direitos fundamentais em risco com essa ampliação, também por meio de uma esfera regulatória processual penal bem-estruturada, mas não exclusivamente (Ramiro *et al*, 2021, p. 3).

O Instituto de Referência em Internet e Sociedade (IRIS-BH), em parceria com o Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec), ofereceu, em 2021, um decálogo de recomendações sobre direitos digitais e produção de

provas em que foram oferecidas recomendações relevantes para iniciativas legislativas. Dentre elas, destaca-se a orientação de que todas as operações de tratamento de dados pessoais para fins de segurança pública e persecução penal devam ser expressamente previstas em lei e vinculadas aos princípios da LGPD, mesmo que não contem ainda com disciplina em lei específica (Ramiro *et al*, 2021, p. 6).

Também existe a recomendação de que dados pessoais tratados no contexto da produção de provas no processo penal devam ser protegidos durante toda a cadeia de custódia com as melhores técnicas de segurança da informação disponíveis, como forma de impedir incidentes de segurança, violação aos direitos dos titulares e comprometimento dos processos investigativos (Ramiro *et al*, 2021, p. 7). Isso além de submissão de atividades investigativas com produção de provas que ofereçam riscos (Ramiro et al, 2021, p. 12) à supervisão e às diretrizes administrativas do Conselho Nacional de Justiça (CNJ).

A regulamentação dos procedimentos investigativos garante maior segurança jurídica e permite que se resguardem as garantias constitucionais e os debates em curso sobre a reforma do CPP são importantes para a garantia dos direitos fundamentais diante das novas tecnologias. Desse modo, importa um diálogo estreito com a disciplina de proteção de dados na esfera das investigações criminais e ampliação dos debates públicos sobre o risco que as ferramentas de exploração de vulnerabilidades e extração de dados (notadamente *hacking* governamental) trazem à sociedade e ao Estado Democrático de Direito como um todo, nos termos da redação atual do projeto.

3

Securitização e vigilância: as duas faces do tecnosolucionismo na segurança pública

Desenvolvimento das tecnologias de segurança no Brasil

O objetivo deste capítulo é apresentar um panorama histórico sobre a utilização da tecnologia na área da segurança pública a nível nacional e, mais detidamente, no município do Rio de Janeiro. Pretendemos contextualizar o leitor acerca das políticas de segurança pública nacionais, suas diretrizes e implementações.

A partir disso, propomos descrever e refletir sobre os dilemas e as perspectivas envolvidas na implementação da tecnologia na área da segurança pública nos dois recortes geográficos citados. Não é nosso objetivo produzir um resgate historiográfico da temática, mas sim traçar um panorama histórico, político e contextual que informe ao leitor sobre nosso campo de estudo.

Dentro dessa proposta, Moema Freire (2009) apresenta um panorama das políticas de segurança pública em cinco décadas: da época da ditadura militar até o ano de publicação de seu artigo em 2009. A autora explica que as ações públicas na área da segurança apresentam variações significativas quanto a objetivos e estratégias ao longo dessas décadas e define o que denomina de três paradigmas principais.

Por paradigma, Freire (2009) compreende a noção de visões de mundo compartilhadas que influenciam as formas de pensar de um grupo em um determinado tempo, não apenas no que se refere ao fazer científico, mas também na produção de políticas públicas. Seriam eles: o paradigma de Segurança Nacional, o de Segurança Pública e o de Segurança Cidadã.

É importante compreendermos a ressalva da autora para a utilização dos "paradigmas" em sua análise. Aqui, ela destaca que não se trata de compreendê-los como categorias rígidas e excludentes de análise da realidade. Os paradigmas podem ter suas características alteradas com o passar do tempo, mas existe um núcleo central — traços mais marcantes e fixos — que permite que cada um deles seja identificado e reconhecido.

Da mesma forma, o paradigma não é sinônimo de política pública, eles são "[…] crenças, valores e conceitos que predominam no governo e na sociedade em determinada localidade e período. Mas isso não quer dizer que essas mesmas crenças, valores e conceitos sejam automaticamente traduzidos em políticas públicas" (Freire, 2009, p. 102).

Assim, o paradigma de Segurança Nacional representa os anos de ditadura militar no Brasil (1964-1985), período em que foram priorizadas a defesa do Estado e a ordem política e social. Essa perspectiva fundamentava-se na lógica da supremacia inquestionável do interesse nacional, definido pela elite no poder. Freire (2009) explica que a atuação do Estado era pautada na Doutrina de Segurança Nacional e Desenvolvimento, criada pela Escola Superior de Guerra. Tal doutrina foi formulada a partir do conceito de Segurança Nacional: a habilidade do Estado em assegurar a obtenção e manutenção de seus objetivos nacionais, apesar das oposições ou pressões existentes ou potenciais.

A noção de defesa nacional estava, portanto, associada à defesa do Estado, princípio contido na Constituição de 1967, cuja Seção V destinava-se à regulamentação da Segurança Nacional. Com o recrudescimento do regime e as mudanças legislativas de 1969, as Forças Armadas ocuparam o lugar de intérpretes da vontade nacional.

Dessa forma, a Segurança Nacional elegeu como prioridade o combate ao inimigo externo, identificado como o comunismo, e ao inimigo interno, qualquer indivíduo ou grupo contrário à ordem vigente. Com uma atuação repressiva contra qualquer um que se opunha aos interesses do Estado, consubstanciado nos interesses daqueles que estavam no poder.

O segundo paradigma de que trata Freire (2009) diz respeito ao momento da redemocratização do Estado brasileiro, representado pela promulgação da Constituição de 1988, que, no art. 144, reconhece a Segurança Pública como dever do Estado, direito e responsabilidade de todos. Aqui, há a preocupação em se diferenciar os papéis institucionais das polícias e do Exército. Sendo as primeiras responsáveis pela segurança pública, assuntos relacionados à violência interna, e o Exército ficando à cargo da segurança nacional, aqui compreendida como as questões externas com relação à soberania nacional e à defesa do território.

Nesse novo paradigma, o da Segurança Pública, os estados passam a ser os principais responsáveis pela gestão das polícias civis e militares. Sobre essa transição de paradigmas, Freire (2009) assim explica:

> Nesse sentido, no paradigma da Segurança Pública, cabe primordialmente às instituições policiais a responsabilidade pelo controle e prevenção da violência. No entanto, enquanto na perspectiva da Segurança Nacional a violência era representada como as ameaças aos interesses nacionais, no arcabouço da Segurança Pública esta é caracterizada como ameaça à integridade das pessoas e do patrimônio (Freire, 2009, p. 105).

Já a terceira perspectiva elencada pela autora diz respeito à Segurança Cidadã, que teria sido criada por volta da segunda metade da década de 1990 com a experiência colombiana. Esse recente paradigma trata a violência por uma abordagem multicausal e defende a atuação do poder público, tanto no controle da violência como na esfera da prevenção, por meio de políticas públicas integradas em âmbitos locais, com uma participação mais engajada dos municípios. Uma atuação baseada nesse paradigma envolve diversas instituições públicas, bem como a participação da sociedade civil, englobando ações em áreas como saúde, educação, lazer, cultura, esporte, entre outras.

Para Freire (2009), existem no Brasil tentativas de aproximação a esse terceiro paradigma. Entre elas, podemos citar o Programa Nacional de Segurança Pública (Pronasci), que foi criado pela Lei n. 11.530/2007 com o objetivo de promover e articular de maneira sistêmica os entes federados e a sociedade na área da segurança pública, principalmente estimulando a participação dos municípios como entes construtores de políticas públicas de segurança.

Kant de Lima, Eilbaum e Pires (2010) também destacam que, desde os anos 2000 no Brasil, a Segurança Pública e a Justiça Criminal têm se constituído temas importantes para a agenda política dos governantes, com a elaboração e implementação, em níveis federal e estadual, de programas de reforma das instituições policiais e judiciárias. Os autores pontuam que esse movimento tem acontecido em toda a América Latina, motivado pela ampliação do acesso à justiça e pela modernização do funcionamento do sistema de segurança. No campo da Segurança Pública, em nível nacional, isso ocorreu com a criação das Guardas Municipais.

Os autores destacam que durante o processo de elaboração da Constituição de 1988, após duas décadas de regime militar, diversas instituições foram repensadas, com foco nos sistemas judiciário e de segurança pública. Debates em torno da eficácia, da eficiência e da efetividade desses campos de atuação do poder público foram intensificados com reformas amplas e generalizadas.

Data desse contexto a criação dos Juizados Especiais, por exemplo, que buscava consolidar uma nova concepção de prestação jurisdicional no país que ampliasse a rede institucional de resolução de conflitos, o que se esperava democratizar o Judiciário. Na área da segurança pública, por sua vez, a Constituição de 1988 criou um sistema hierarquizado de instituições separadas para o exercício das atividades de patrulhamento ostensivo e investigação, as polícias militar e civil, respectivamente. Os autores explicam que o texto normativo não

se dedicou a integrar as práticas de investigação às de patrulhamento, o que resultaria, atualmente, em mecanismos de disputas entre as corporações, que pouco ou nada contribuem para uma atuação preventiva à violência e ao cometimento de delitos.

Apesar da previsão constitucional inovadora da criação das Guardas Municipais, Kant de Lima, Eilbaum e Pires (2010) argumentam que a Constituição de 1988 implementou uma perspectiva descentralizadora e socialmente participativa, principalmente, nas áreas de educação e saúde. Mas, no que concerne à Segurança Pública, essas iniciativas foram mínimas, pois o protagonismo de intervenção na violência e na criminalidade teria sido outorgado quase totalmente às polícias estaduais.

Porém, antes de nos dedicarmos propriamente à análise dessas mudanças legislativas, é relevante abordarmos os diversos Planos Nacionais de Segurança Pública implementados desde o segundo governo do presidente Fernando Henrique Cardoso (FHC).

Os planos nacionais de segurança pública

No contexto pós-Constituição de 1988, o Governo Federal estava lidando com a tarefa de elaborar uma Política Nacional de Segurança Pública para criar diretrizes de articulação, coordenação e sistematização das diversas ações nesse campo (Delgado, 2021). Conforme descreve Soares (2007), sucessivos ministros da Justiça, com a colaboração de secretários nacionais de segurança, se empenharam lentamente para isso durante o governo FHC (1995-2003). Até que, no dia 12 de junho de 2000, ocorreu no Rio de Janeiro o dramático caso do sequestro do ônibus 174, episódio retratado em um documentário de José Padilha intitulado *Ônibus 174*.

Sandro Barbosa do Nascimento, sobrevivente do massacre da Candelária, sequestra o ônibus intermunicipal 174 e toma os passageiros como reféns. Com cobertura integral da mídia, a população pôde acompanhar a tragédia pela televisão. Após horas de negociação malsucedida com a polícia, o sequestrador desceu do ônibus usando uma mulher de escudo. Ao tentar alvejar Sandro, um dos atiradores do Batalhão de Operações Especiais da Polícia Militar (Bope) erra e acerta a vítima que recebe ainda três disparos do sequestrador e morre no local. Logo em seguida, Sandro é imobilizado e morto por asfixia dentro da viatura policial.

Devido à repercussão nacional do caso, uma vez que a sociedade assistia a tudo ao vivo, o então presidente da República determinou que o Plano Nacional de Segurança fosse publicado com as diretrizes de qual seria a agenda nacional para a segurança. Uma semana após o caso do ônibus 174, o Plano Nacional seria publicado. Sobre isso Soares (2007) explica que "em uma semana, a nação conheceria o primeiro plano de segurança pública de sua história democrática recente, o qual, em função do parto precoce, precipitado a fórceps, vinha a público sob a forma canhestra de listagem assistemática de intenções heterogêneas" (Soares, 2007, p. 83).

Assim, o primeiro Plano Nacional de Segurança Pública foi uma resposta reativa à opinião pública diante de um episódio de violência de grande repercussão, de caráter muito mais político do que estratégico. Tendo se caracterizado por uma elevada capacidade de formulação de políticas, mas de baixa capacidade de implementação (Delgado, 2021). Soares (2007) chama a atenção para o caráter dispersivo e assistemático desse plano.

Não obstante essas críticas, Soares (2007) afirma que o governo FHC representou uma virada positiva, democrática e progressista na forma como politicamente lidávamos com a segurança pública no Brasil. Segundo o autor, a questão da segurança pública ganhou status político superior, além de ter sido reconhecida a responsabilidade do Governo Federal sobre essa matéria. Outro ponto positivo foi que o governo FHC firmou um compromisso político com a agenda dos Direitos Humanos, mais especificamente na área da Segurança Pública.

O segundo Plano Nacional de Segurança Pública foi apresentado à população pela primeira vez, ainda nas eleições presidenciais, pelo então candidato Luiz Inácio Lula da Silva. De acordo com Soares (2007), o plano foi bem recebido até mesmo por adversários políticos, devido ao seu compromisso com a seriedade técnica e sua posição não partidária, que busca a construção de um mínimo consenso nacional. O documento partia do pressuposto de que a segurança pública é questão de Estado, e não de governo.

Os principais objetivos desse segundo Plano eram reformar as instituições de segurança pública e implementar o Sistema Único de Segurança Pública (SUSP). O SUSP pretende integrar a troca de informações entre as instituições de segurança e a articulação entre elas e a sociedade civil. Nesse novo modelo, conforme Soares (2007), o trabalho policial seria orientado principalmente para a prevenção, articulando-se com políticas sociais preventivas.

Todavia, de acordo com Delgado (2021), o plano não se efetivou, pois enfrentou oposições políticas e, após um ano, foi abandonado pelo Governo Federal. Soares (2007) argumenta nesse mesmo sentido ao explicar que o Governo Federal não cumpriu com os compromissos programados e, ao invés disso, deslocou o Plano Nacional do centro da agenda do Ministério da Justiça, substituindo-o por ações da polícia federal, que passaram a representar a imagem de uma atividade competente e destemida à sociedade.

Além disso, o autor acrescenta que:

> Não é preciso ponderar, entretanto, que, por mais virtuosas que tenham sido as operações da polícia federal — surgiram questionamentos pertinentes quanto à consistência de algumas e ao caráter midiático de muitas delas —, ações policiais não podem substituir uma Política de Segurança Pública (Soares, 2007, p. 91).

Soares (2007), que participou da elaboração do Plano Nacional de Segurança Pública no primeiro governo Lula, tendo deixado seu cargo na Secretaria Nacional de Segurança Pública (Senasp) em outubro de 2003, avalia da seguinte forma os compromissos assumidos e desenvolvidos pelo Plano que, todavia, nunca saíram do papel:

> A armadilha política descrita antes, fruto da contradição entre o ciclo eleitoral e o tempo de maturação de políticas públicas reformistas, terminou levando o governo federal a aposentar, precocemente, seus compromissos ambiciosos na segurança pública: o Plano Nacional foi deslocado, progressivamente, do centro da agenda do Ministério da Justiça, e substituído, gradualmente, por ações da polícia federal, que passaram a emitir para a sociedade a mensagem de atividade competente e destemida, na contramão de nossa tradicional e corrosiva impunidade. Não é preciso ponderar, entretanto, que, por mais virtuosas que tenham sido as operações da polícia federal surgiram questionamentos pertinentes quanto à consistência de algumas e ao caráter midiático de muitas delas, ações policiais não podem substituir uma Política de Segurança Pública. Sobretudo em uma situação como a brasileira, marcada por fragmentação institucional e pela incompatibilidade entre o modelo herdado da ditadura e os desafios crescentes de uma sociedade que se complexifica e transnacionaliza, em contexto democrático, mas profundamente desigual (Soares, 2007, p. 93).

No segundo governo Lula, observamos a continuidade da construção de uma Política Nacional de Segurança Pública (Delgado, 2021) por meio do lançamento do Programa Nacional de Segurança Pública com Cidadania (Pronasci), em agosto de 2007. Este documento valoriza a contribuição dos municípios para a Segurança Pública (Soares, 2007). Conforme Delgado (2021), o Pronasci é o principal símbolo do tratamento político dado à segurança pública pelo segundo mandato do presidente Lula. Tinha caráter preventivo, com especial atenção aos jovens residentes em áreas vulneráveis.

O Pronasci implicou, conforme Kopittke (2017), um grande crescimento no valor dos recursos destinados pelo Governo Federal às políticas de segurança, com incremento de R$ 1,2 bilhão ao ano entre 2007 e 2011. De acordo com o autor, o programa se caracterizou por atribuir prioridade ao papel dos municípios na segurança pública, criando gabinetes de gestão integrada dos municípios, além do grande investimento em formação policial, com a criação de uma diversa gama de cursos.

Todavia, Kopittke (2017) ressalta que o Pronasci não teria criado nenhuma estrutura permanente e que os avanços orçamentários e conceituais foram desfeitos no início do governo Dilma, em 2011, que reorientou a política para o modelo da segurança nacional.

Vale destacar que, no período de implementação do Pronasci, houve a remodelação do Conselho Nacional de Segurança Pública (Conasp), por meio de uma Conferência Nacional de Segurança Pública, em 2009, com a participação de mais de 250 mil pessoas (Kopittke, 2017). Apesar da inclusão da sociedade civil e de outros atores no Conasp, ele não recebeu poderes deliberativos nem foi vinculado à gestão do Fundo Nacional, portanto, esvaziado de qualquer poder de fato.

Já durante os governos Dilma, foram priorizadas estratégias de segurança sobre as fronteiras e a delegação de poderes às Forças Armadas na área de segurança pública. Sobre esse período, Kopittke (2017) destaca a aprovação da lei que criou o Sistema Nacional de Informações de Segurança Pública, Prisionais e sobre Drogas (Sinesp) e o Estatuto da Guardas Municipais, todavia também esvaziados de qualquer estrutura institucional e, em razão disso, incapazes de realizar mudanças estruturais.

Fabio de Sá e Silva (2017) explica que, em meados de 2012, o Ministério da Justiça passou a divulgar um novo Plano Nacional de Segurança Pública que

reunia três novidades: a primeira era com relação à própria agenda federal, agora mais direcionada ao crime organizado, ao uso de drogas, ao sistema prisional e à segurança de grandes eventos do que com a prevenção e redução de manifestações mais cotidianas da violência urbana, como homicídios, roubos e furtos.

A segunda novidade abarcava as relações entre entes federados em que se destacavam as competências executivas dos estados e da União. Os municípios, as guardas municipais e os projetos de prevenção ou projetos sociais, em que a gestão costuma ser, em geral, municipal, ocupam posição discreta se comparados ao Pronasci do governo Lula.

Por sua vez, o combate ao crime organizado, a segurança nas fronteiras e a segurança de grandes eventos foram direcionados para serem geridos por organizações federais, como o Exército, polícias federais e o Ministério Público Federal. Já o Brasil Mais Seguro, programa de enfrentamento à violência, envolvia o fortalecimento da polícia civil e da perícia, organizações tipicamente estaduais.

A contradição disso tudo reside no fato de que o Plano Nacional partia da concepção de que o Governo Federal desempenharia apenas função de apoio aos estados na produção e gestão das ações de segurança pública. Assim, conforme afirma Fabio de Sá e Silva (2017), percebemos como, durante o primeiro governo de Dilma Rousseff, a segurança pública voltava a ganhar conotação policial e estadual, com a atuação pontual e fragmentada da União.

Mathias, Zague e Santos (2019), em artigo que analisa a operacionalização das Forças Armadas ao longo do governo Dilma Rousseff, concluem que:

> O ponto mais importante do que aqui foi apresentado é o perceptível aprofundamento da militarização da segurança pública no governo rousseff, representado especialmente pela maior presença das forças armadas nas atividades policiais cotidianas. portanto, não é um equívoco dizer que sua política militar, isto é, de emprego das forças armadas, se resume ao cumprimento de missões no âmbito da segurança interna. Mesmo quando se trata da atividade precípua de defesa, ou seja, atuação militar externa, esta tem como objetivo o treinamento para a garantia da lei e da ordem, como se mostra pela participação na minustah (Mathias; Zague; Santos, 2019, p. 163).

No segundo mandato, ocorreram discussões e reuniões para a elaboração de um novo plano de segurança pública que contemplasse e resolvesse

os problemas do anterior. Contudo, ante a falta de avanço do Ministério da Justiça e o impedimento político da presidenta em 2016, Michel Temer assumiu a presidência, imprimindo uma nova direção à política de segurança pública no país.

Em 2017, diante de uma grave crise no sistema prisional das regiões Norte e Nordeste, Temer lança o novo Plano Nacional de Segurança Pública. Fabio de Sá e Silva (2017) analisa que este documento repete grande parte dos erros dos planos antecessores, mas que duas características merecem destaque: a primeira trata da ampliação das capacidades executivas do Governo Federal, por exemplo, com a construção de cinco presídios federais.

A segunda diz respeito à ênfase na abordagem repressivo-ostensiva, já anunciada em agosto de 2016 pelo Ministro da Justiça, Alexandre de Moraes, ao afirmar que o Brasil precisava de "menos pesquisa e mais armamento" (Silva, 2017, p. 24).

Este Plano, criado e implementado no governo Temer, foi objeto de muitas críticas tanto de pesquisadores e acadêmicos da área da segurança pública quanto de segmentos da sociedade civil, incluindo os próprios policiais, que não foram chamados para participar das discussões de elaboração do projeto.

Em 2018, foi criado o Ministério da Segurança Pública, com o objetivo de promover a integração das forças policiais e aprovada a Lei n. 13.675/18, que criou o Conselho Nacional de Segurança Pública e Defesa Social e disciplinou sobre a organização e o funcionamento dos órgãos responsáveis pela segurança pública. A lei instituiu um plano nacional que teria duração de dez anos, elaborando um planejamento com propostas a curto e médio prazos, com a ressalva de uma atuação coordenada e integrada dos órgãos de segurança pública, com o envolvimento do governo federal (Spaniol, Júnior e Rodrigues, 2020).

Também em 2018 ocorreu a intervenção federal militar no Rio de Janeiro, o que, segundo Souza e Serra (2020), foi um movimento de fortalecimento do militarismo no Brasil. De acordo com os autores, a intervenção foi uma política espalhafatosa do ponto de vista dos gastos públicos e de ostentação de força militar, mas que, na prática, resultou em uma política ineficiente para a redução das taxas de violência urbana no Rio de Janeiro. Sobre a intervenção no Rio de Janeiro e a militarização da política de segurança pública no país, autores argumentam que:

> A intervenção, neste sentido, não apenas serviu de laboratório para medidas repressivas e violentas de segurança, como também foi um teste de legitimação da gestão militarizada da segurança pública, com seu componente de construção permanente de um inimigo a ser abatido, dentro da lógica da guerra e do confronto armado. A intervenção de 2018 não é fato novo. Foram várias intervenções, e em nenhuma os objetivos alegados foram atingidos. Tomam-se aqui as intervenções no Rio de Janeiro porque são exemplares em relação à militarização e ao aumento da violência do Estado. Grande parte das justificativas para as intervenções gira em torno da chamada guerra ao crime organizado e ao tráfico de drogas. Ao longo da última década, o estado recorreu às forças armadas pelo menos doze vezes (Souza e Serra, 2020, p. 213).

Feitas essas considerações sobre as políticas de segurança pública no Brasil para a devida contextualização do leitor a respeito de como se tem pensado e gerido a questão da segurança pelos diferentes governos, é importante ressaltar ainda a importância dos megaeventos no país para a intercessão entre os campos da segurança pública, da tecnologia e da integração. Para pensar esse ponto, apresentamos no próximo tópico uma análise sobre os megaeventos e a política de segurança pública no estado do Rio de Janeiro, principalmente, no que concerne ao uso de tecnologias, por compreendermos, assim como Cardoso (2019), que, apesar das particularidades do caso, este é um estado que possibilita aproximações com a política nacional de segurança pública.

O Rio de Janeiro e os megaeventos

Entre 2013 e 2018, o Rio de Janeiro foi palco de um ciclo de megaeventos, como a Copa do Mundo de Futebol, os Jogos Olímpicos e a Jornada Mundial da Juventude Católica, que trouxe o Papa Francisco ao Rio de Janeiro. Além disso, a cidade experimentou uma grande política de ocupação territorial permanente das favelas e foi colocada várias vezes, em diferentes escalas, sob intervenção militar das Forças Armadas.

No caso do Brasil, por diversas razões, o legado dos megaeventos estaria relacionado à ampliação da segurança pública no combate à violência urbana. Além disso, conforme Cardoso (2019), em todas essas situações, aquilo que se convencionou chamar de “centro integrado de comando e controle” teria participado no planejamento ou na execução.

Assim, desde o planejamento estratégico para a segurança durante os megaeventos, foi anunciado que os dois grandes legados securitários seriam a construção de um sistema integrado de comando e controle nacional e, com isso, a elaboração de um novo paradigma de atuação das forças de segurança e defesa, que se pautava em operações coordenadas e integradas pelas diferentes agências indireta ou diretamente envolvidas. No Rio de Janeiro foi então construído o maior prédio de Comando e Controle Integrado do país — deixado sob o comando da polícia militar — constituindo grande investimento na área de segurança e tecnologia para atuar na redução das taxas de violência urbana.

Todavia, como é possível imaginar, essa última tarefa seria um grande desafio, tendo em vista que nossa segurança pública tem uma estrutura fragmentada. Considerando-se apenas as forças policiais, temos, a nível estadual, as polícias militar e civil e, em âmbito nacional, a polícia federal e a polícia rodoviária federal, além da Força Nacional de Segurança. Da mesma forma, as esferas de segurança pública e ordenamento urbano se confundem, e as guardas municipais ganham características de polícia militar (Cardeal e Ribeiro, 2017).

Kant de Lima, Eilbaum e Pires (2010) ressaltam que, por motivos históricos, desde os anos de 1980, as atividades policiais são bem demarcadas no estado do Rio de Janeiro entre atividade ostensiva e atividade investigativa, ficando a primeira a cargo da polícia militar e a segunda sob responsabilidade da polícia civil, o que faz com que o patrulhamento urbano seja hegemonicamente um trabalho da polícia militar.

Divisões estruturais com características tão fragmentárias geram problemas como a criação de bancos de dados separados que, muitas vezes, não se comunicam ou sequer se conhecem, a realização de tarefas redundantes, a competição institucional por prestígio, recursos, reconhecimento e atribuições, além do represamento de informações que possam ser consideradas, sob algum aspecto, “valiosas”, de acordo com Bruno Cardoso (2019).

Portanto, um planejamento que objetive a coordenação e a integração entre as diferentes instituições envolvidas na segurança pública é, sob vários aspectos, por exemplo, estrutural, mas também, do ponto de vista dos hábitos de trabalho dos atores envolvidos com fazer da segurança pública, um desafio.

Bruno Cardoso (2019) identifica o incremento de uma rede sociotécnica que reforça um modelo de segurança pública, que o autor denomina de “modelo gerencial-militarizado”, como forma principal de planejamento da segurança no

Rio de Janeiro. Este modelo se caracteriza pela junção de duas lógicas: a lógica gerencial, que desde a década de 1980 se expande na burocracia do estado brasileiro, com uma ideia de aproximar a organização do Estado a uma empresa privada, com valores em torno de uma gestão do estado voltada para o campo mais da administração de empresas do que das noções de correntes em ciências sociais ou visões clássicas da ciência política. A racionalidade empresarial é alçada ao horizonte de ação a ser buscado.

A segunda lógica é a militarizada, que, por sua vez, está associada à organização da segurança pública em torno de um CICC. O autor destaca, por exemplo, que durante a intervenção militar, o prédio foi utilizado como quartel-general de generais do Exército brasileiro para gerir parte significativa do estado do Rio de Janeiro, transmitindo a ideia de que fazer segurança pública envolve pensar o espaço da cidade como um território em guerra (Cardoso, 2019).

Esta breve contextualização sobre as políticas de segurança pública buscou contribuir para a reflexão sobre a interseção atual entre tecnologia e segurança pública no que diz respeito às práticas cotidianas de trabalho dos atores que atuam nessas instituições.

4

Mapeamento do cenário brasileiro no uso da tecnologia pelas forças de segurança

Mapeamento do panorama nacional

O mapeamento dos usos de tecnologia na segurança pública no território brasileiro utilizou metodologia exploratória, combinando pesquisa empírica a partir de dois métodos principais: o primeiro dedicado a entrevistas com agentes de segurança no Estado do Rio de Janeiro e o segundo aplicando análise documental sobre reportagens e publicações de grande circulação sobre o uso de tecnologias baseadas em dados pelas forças de segurança pública no Brasil.

Optou-se por esse método de pesquisa tendo em vista que, na etapa de levantamento bibliográfico, que perdurou doze meses, notou-se não apenas a presença de poucos estudos teóricos sobre o tema no país como um reduzido contingente de informações suficientemente disponíveis ao público sobre os usos e contratações de tecnologias para as forças de segurança, nas suas mais diversas frentes de atuação. Mais precisamente, em números: tipos de tecnologia, quantidade adquirida ou mesmo seus valores e custos.

Nesse sentido, tomou-se como ponto de partida para compreensão do panorama nacional o próprio foco de investigação da pesquisa: as percepções pessoais dos agentes de segurança. As entrevistas serviriam como premissas para, em um primeiro momento, não apenas compreender o cotidiano e a trajetória dos agentes entrevistados, mas também ter uma oportunidade de obter acesso a documentos oficiais referentes a compra, aquisição ou mesmo os simples usos de aparatos tecnológicos de toda sorte.

Logo notou-se que o acesso a tais instrumentos não seria tão facilmente cedido, haja vista o caráter sigiloso que permeia não apenas as investigações criminais como um todo, mas também o próprio funcionamento institucional a respeito do compartilhamento de informações internas para externos, ainda que comprometidos com fins exclusivamente acadêmicos.

Foram compiladas e analisadas vinte e três entrevistas com atores-chave das forças de segurança na cidade do Rio de Janeiro, de modo a identificar alguns dos principais tipos de tecnologia empregados e citados em sede de entrevistas. Com base na recorrência dos aparatos tecnológicos citados nas falas dos entrevistados, realizou-se um mapeamento de notícias de abrangência nacional sobre o uso de novas tecnologias pelos órgãos de segurança pública no Brasil.

As tecnologias que foram citadas de maneira mais recorrente foram: câmeras corporais (*bodycams*), drones, reconhecimento facial e reconhecimento óptico de caracteres (OCR) para leitura de placas veiculares. Buscou-se mapear todas as notícias existentes sobre o tema no Brasil dentro do critério temporal de primeiro de junho de 2021, data em que a pesquisa teve início, até 31 de maio de 2022, respeitando o cronograma de trabalho de um ano para levantamento e monitoramento de dados, além de análise bibliográfica.

A seleção de mídia utilizou a ferramenta computacional *Media Cloud* para captura de notícias e extração de características semânticas dos textos, agrupando-as em duas coleções: Brazil-National, englobando 86 fontes de nível nacional, e Brazil-State & Local, que abarcou 1.429 fontes, como jornais, revistas e portais de abrangência estadual, referentes a todos os estados brasileiros.

Foram obtidos 3.609 resultados, com exclusão de 1.197 resultados duplicados. Desse modo, foram submetidos à análise manual dos pesquisadores do projeto 2.412 resultados, a partir de um formulário desenvolvido internamente no programa *Google Sheets*. Nesta etapa de mapeamento nacional, os pesquisadores realizaram a leitura de cada um dos resultados de maneira detida, buscando extrair informações sobre o tipo de tecnologia empregada, o âmbito de aplicação (federal, estadual ou municipal), bem como o órgão de segurança pública responsável pela utilização da tecnologia apresentada.

Em termos quantitativos, esta etapa de pesquisa permitiu identificar em que regiões do Brasil há aplicação pelas forças de segurança de cada um dos tipos de tecnologia mencionados nas notícias. No caso do reconhecimento facial, os estados do Acre, Amazonas, Roraima, Pará, Bahia, Minas Gerais, Goiás, Espírito Santo e Paraná despontaram como aqueles citados no contexto de adoção da tecnologia.

No estado do Acre, foi apresentado o plano municipal "Rio Branco mais segura", em fevereiro de 2022, com foco na instalação de 430 câmeras de videomonitoramento na cidade, dentre as quais dezoito terão tecnologia de reconhecimento facial, com instalação prevista até o final do ano de 2022 (Brasil, 2022). Em sua primeira etapa de instalação, estão previstos espaços públicos de grande circulação, como o centro da cidade, além da Regional da Seis de Agosto, Parque Chico Mendes, Rodoviária Internacional de Rio Branco e o Horto Florestal.

Figura 4.1 Estados brasileiros que utilizam reconhecimento facial.

No Amazonas, o reconhecimento facial para emissão de carteira nacional de habilitação já é uma realidade desde 2019,[10] e o uso do mesmo para identificar foragidos da justiça com mandado de prisão em aberto a partir dos aparelhos celulares de policiais militares foi desenvolvido em meados de 2020. O intuito era subsidiar a atuação dos policiais nas ruas, economizar custos e auxiliar no aumento de produtividade nas operações contra a criminalidade.[11]

---

10 Cf. http://www.ssp.am.gov.br/reconhecimento-facial-para-emissao-da-cnh-e-implantado-no-amazonas/reconhecimento-facial-para-emissao-da-cnh-e-implantado-no-amazonas-5/.

11 Cf. PM do Amazonas desenvolve tecnologia de reconhecimento facial de foragidos pelo celular. **Informe Amazonas**. 17 nov. 2021. Disponível em: <https://informeamazonas.com.br/pm-do-amazonas-desenvolve-tecnologia-de-reconhecimento-facial-de-foragidos-pelo-celular/>. Acesso em: 06 ago. 2022.

A tecnologia é o aplicativo Comando Operacional da Polícia Militar do Amazonas (Copmam), encomendado pelo comandante-geral da polícia militar, coronel Ayrton Norte, voltado para serviços operacionais dos policiais militares e restrito para as forças de segurança. O aplicativo estava em fases de teste em 2020, mas, a despeito da intensa busca e levantamento de notícias, não foram encontradas novas informações capazes de atualizar o status de incorporação efetiva, ou não, da tecnologia nas operações policiais.

Até abril de 2021, havia 41 câmeras de reconhecimento facial nas ruas de Manaus, cuja aquisição foi realizada com recurso federal por meio do Financiamento à Infraestrutura e ao Saneamento (Finisa), após licitação em que foi vencedora a empresa Motorola Solution LTDA. O custo total foi de R$ 2.994.820, com responsabilidade de instalação e manutenção pelo prazo de um ano (Elander, 2021). Estimavam-se 180 câmeras de monitoramento até o final de 2021, mas não foram encontrados dados atualizados sobre a efetivação desse aumento de contingente tecnológico.

Outros levantamentos merecem destaque sobre reconhecimento facial no Amazonas e podem ser relevantes para tessituras no campo da segurança pública. Dentre eles, a existência de uma Lei Municipal em Manaus, em vigor, que dispõe sobre a incorporação do sistema de identificação biométrica facial na fiscalização do uso de transporte coletivo urbano de passageiros (Lei 2.474/19) e a adoção de ponto eletrônico com reconhecimento facial pela prefeitura de Manaus em abril de 2022, para o alegado aumento do rigor na fiscalização dos serviços oferecidos pela gestão municipal.[12]

Roraima possui uma situação geográfica sensível no contexto brasileiro de combate à violência e de guerra às drogas na região das fronteiras com Venezuela e Guiana. Na região norte do estado, já são utilizados equipamentos na cidade de Pacaraima cujo custo de instalação foi estimado em 3,1 milhões de reais, oriundos do projeto Fronteira Tech: uma parceria entre o governo do estado e a Agência Brasileira de Desenvolvimento Industrial (ABDI). Ao todo, foram instaladas vinte luminárias inteligentes com câmera de vigilância, software de reconhecimento facial, um datacenter para armazenamento e processamento

12 Cf. PREFEITURA de Manaus vai adotar ponto eletrônico com reconhecimento facial. **Em Tempo**. Serviço Público. 29 abr. 2022. Disponível em: <https://emtempo.com.br/38293/amazonas/prefeitura-de-manaus-vai-adotar-ponto-eletronico-com-reconhecimento-facial/>. Acesso em: 06 ago. 2022.

de imagens e dados, telas de *videowall*, quatro câmeras de reconhecimento de placas de veículos, e também drones com câmera termográfica.[13]

O estado do Pará já emprega biometria facial nos transportes coletivos de Belém desde 2019 para aferição de gratuidades e benefícios (Pelegi, 2022), emprega sistema de reconhecimento facial para os serviços de Carteira Nacional de Habilitação (CNH) pelo Detran e conta com tecnologia de acesso biométrico facial em todas as unidades prisionais do estado desde janeiro de 2022,[14] quando apresentada pela Secretaria do Estado de Administração Penitenciária (Seap) como forma de fortalecer o controle de acesso, segurança e circulação de policiais, colaboradores, internos, advogados e visitantes.

A Bahia foi o primeiro estado no Brasil a utilizar o sistema de reconhecimento facial de modo experimental, em dezembro de 2018, o que atualmente já auxiliou a prisão de 351 pessoas.[15] Já são 78 municípios que contam com serviços de reconhecimento facial, de placas e de análise situacional, com 1.200 câmeras em Salvador e região metropolitana, por meio da Secretaria de Segurança Pública (SSP).[16] Os novos equipamentos tiveram investimento de 665 milhões de reais em 2022, ampliando a cobertura do sistema de monitoramento na capital, que já contava com trezentas unidades.

Goiás tem se mostrado um forte entusiasta dos sistemas de reconhecimento facial, aplicando-os não somente nas escolas e Centros Municipais de Educação Infantil (CMEIs) de Goiânia, com o Programa Conecta Educação, desde outubro de 2021 (Alves, 2021), como também se escusado de participar de iniciativas legislativas e movimentos parlamentares que confrontam os riscos dos usos da tecnologia nos espaços públicos (Mariano, 2022).

---

13 Cf. RORAIMA instala câmeras de monitoramento na fronteira do Brasil com a Venezuela. **Segurança eletrônica**, 2022. Disponível em: <https://revistasegurancaeletronica.com.br/roraima-instala-cameras-de-monitoramento-na-fronteira-do-brasil-com-a-venezuela/>. Acesso em: 06 ago. 2022.

14 Cf. Seap lança sistema de reconhecimento facial para segurança no sistema penitenciário. **O Impacto**. 28 jan. 2022. Disponível em: <https://oimpacto.com.br/2022/01/28/2seap-lanca-sistema-de-reconhecimento-facial-para-seguranca-no-sistema-penitenciario/>. Acesso em: 06 ago. 2022.

15 Contagem datada de 7 de agosto de 2022. Cf. MAIS três foragidos são presos após reconhecimento facial em Salvador e RMS. **Correio 24 horas**. 07 ago. 2022. Disponível em: <https://www.correio24horas.com.br/noticia/nid/mais-tres-foragidos-sao-presos-apos-reconhecimento-facial-em-salvador-e-rms/>. Acesso em: 07 ago. 2022.

16 Cf. GOVERNO do Estado instala 1200 novas câmeras de reconhecimento facial. **Bahia Econômica**. 14 jun. 2022. Disponível em: <https://bahiaeconomica.com.br/wp/2022/06/14/governo-do-estado-instala-1-200-novas-cameras-de-reconhecimento-facial/>. Acesso em: 07 ago. 2022.

Em Minas Gerais, o Tribunal de Justiça do Estado implantou desde 2018 o sistema de reconhecimento facial da Biomtech para cadastramento e apresentação de sentenciados para informação de atividades, dentre os quais presos domiciliares, e aqueles sob suspensão condicional da pena e do processo. O sistema já cadastrou mais de sete mil sentenciados na Vara de Execuções Penais e na 5ª Vara Criminal de Belo Horizonte (Pederzoli, 2019).

Além disso, Minas também conta com sistema de reconhecimento facial de condutores (CNH) desde 2019[17] e implementa biometria facial no estádio do Mineirão, enquanto Belo Horizonte, desde março de 2022, o faz para identificação de pessoas com mandado de prisão em aberto na justiça. O sistema foi desenvolvido por uma empresa mineira de tecnologia, e há promessas de ampliação de uso para substituição de ingresso pelo uso do sistema na entrada.[18]

Já o estado do Paraná tem reconhecimento facial em Curitiba e em Maringá, duas cidades expoentes no uso de tecnologias de reconhecimento facial na segurança pública. Curitiba conta com o Projeto Muralha Digital, lançado em junho de 2020, com novas 488 câmeras de videomonitoramento em pontos estratégicos da cidade e equipamentos de alta resolução full HD, que incluem câmeras de reconhecimento facial, panorâmicas, térmicas e com reconhecimento de placas de veículos, que se somam às cerca de setecentas câmeras já existentes em ruas e estações-tubo.[19]

Maringá, por sua vez, foi considerada a cidade mais inteligente do estado no ano de 2021 e a nona do país. Em 2022, durante a Expoingá, foi apresentada ao público a sua nova aquisição: o Centro de Controle Integrado da Cidade, com sistema de videomonitoramento adquirido recentemente, que está em processo de testes e implementação gradual. Ele será instalado na cidade de Maringá e

---

17 Cf. POLÍCIA Civil apresenta novo sistema de reconhecimento facial de condutores. **Detran MG**. 07 nov. 2019. Disponível em: <https://www.detran.mg.gov.br/sobre-o-detran/sala-de-imprensa/noticias/policia-civil-apresenta-novo-sistema-de-reconhecimento-facial-de-condutores>. Acesso em: 07 ago. 2022.

18 Cf. MINEIRÃO inaugura reconhecimento facial para coibir violência. **Sou BH**. 06 mar. 2022. Disponível em: <https://soubh.uai.com.br/noticias/variedades/mineirao-inaugura-reconhecimento-facial-para-coibir-violencia>. Acesso em: 07 ago. 2022.

19 Cf. CIDADE terá câmeras de reconhecimento facial em pontos estratégicos. Curitiba: **Muralha Digital**. Prefeitura Municipal de Curitiba, 29 jun. 2020. Disponível em: <https://www.curitiba.pr.gov.br/noticias/cidade-tera-cameras-com-reconhecimento-facial-em-pontos-estrategicos/56463>. Acesso em: 07 ago. 2022.

possui capacidade de reconhecimento e identificação facial, além de reconhecimento e leitura de placas de veículos, software de processamento de dados, análises forenses e big data (Herrero, 2022).

No contexto político, são frequentes as disputas envolvendo a legalização e o banimento do reconhecimento facial na segurança pública. Foi movimentada a campanha nacional "Tire Meu Rosto da Sua Mira", capitaneada por dezenas de organizações da sociedade civil e ativistas de direitos humanos e dedicada a influenciar políticas públicas para a proibição e interrupção de projetos que utilizem a tecnologia para fins de segurança pública.

Dentre outras propostas e atividades, a campanha também realizou um mapeamento de iniciativas de projetos de lei sobre o tema em todos os estados da federação, tanto aqueles que fossem pró-banimento quanto os pró-implantação. Totalizando, até a data de quatorze de agosto de 2022, 68 projetos de lei favoráveis ao uso.[20]

Nesse sentido, outra iniciativa da sociedade civil que merece destaque é intitulada "Sai da Minha Cara". Apresentada em 21 de junho de 2022, a proposta incluiu mais de cinquenta parlamentares de diferentes partidos para apresentação de projetos de lei pelo banimento do reconhecimento facial em espaços públicos, demonstrando um movimento multipartidário sobre o caráter alegadamente invasivo e discriminatório dessa tecnologia quando aplicada para fins de segurança pública.[21]

Dentre os estados que utilizam OCR, destacam-se: (i) na região norte, Amazonas e Pará; (ii) na região centro-oeste, Mato Grosso, Mato Grosso do Sul e Goiás; (iii) na região sudeste, São Paulo, Minas Gerais, Rio de Janeiro e Espírito Santo e (iv) na região sul, Paraná, Santa Catarina e Rio Grande do Sul.

---

20 Cf. TIRE meu rosto da sua mira. Mapeamento dos projetos de lei sobre reconhecimento facial nos Estados brasileiros. 2022. Disponível em: <https://tiremeurostodasuamira.org.br/mapeamento/>. Acesso em: 26 jan. 2023.

21 Cf. PARLAMENTARES de todas as regiões do Brasil apresentam projetos de lei pelo banimento do reconhecimento facial em espaços públicos. Instituto Brasileiro de Defesa do Consumidor — Idec. São Paulo, 20 jun. 2022. Disponível em: <https://idec.org.br/release/parlamentares-de-todas-regioes-do-brasil-apresentam-projetos-de-lei-pelo-banimento-do>. Acesso em: 26 jan. 2023.

Figura 4.2 Estados brasileiros que utilizam OCR.

A tecnologia de OCR, ou *Optical Character Recognition*, se aplica para reconhecimento de texto dentro de imagens, tais como fotos e documentos digitalizados. É utilizada para converter virtualmente qualquer tipo de imagem contendo texto, seja ele digitado, manuscrito ou impresso, em versões de dados legíveis por máquina (Kovacs, 2022).

O OCR é uma tecnologia considerada simples que, no contexto de um cercamento eletrônico, pode ser instalado em câmeras de monitoramento das cidades com o objetivo de captar informações. Dentre eles, o uso mais comum é para placas de veículos, em que a tecnologia faz a leitura de caracteres, transformando o conteúdo em texto e o submetendo ao cruzamento de informações com o banco de dados da polícia para identificar padrões, no caso, as infrações.[22]

22 Cf. COMO FUNCIONA O OCR, a tecnologia usada no cercamento eletrônico. Portal da segurança pública. **Blog**. 12 abr. 2021. Disponível em: <https://segpublica.com.br/como-funciona-o-ocr-a-tecnologia-usada-no-cercamento-eletronico/>. Acesso em: 07 ago. 2022.

No cercamento eletrônico, caso as informações de uma placa de veículo sejam capturadas e for reconhecida alguma irregularidade, tal como a adulteração de uma placa ou violações de trânsito, ou mesmo ocorrências de furtos e roubos, um alerta é emitido em tempo real a partir do cruzamento de informações junto ao banco de dados.

Outra tecnologia presente nas investigações criminais, de acordo com o levantamento noticiário apontado, são os drones. Dentre os 26 estados brasileiros e Distrito Federal, apenas nove não foram apontados como utilizadores dessa tecnologia. Na região norte, utilizam a tecnologia, Acre, Amazonas, Rondônia e Pará. Na região nordeste, Piauí, Ceará, Alagoas e Bahia. Na região centro-oeste, todos a utilizam, Mato Grosso, Mato Grosso do Sul, Goiás e o Distrito Federal. Na região sudeste, também todos a utilizam, São Paulo, Minas Gerais, Rio de Janeiro e Espírito Santo. E na região Sul, apenas Paraná e Rio Grande do Sul.

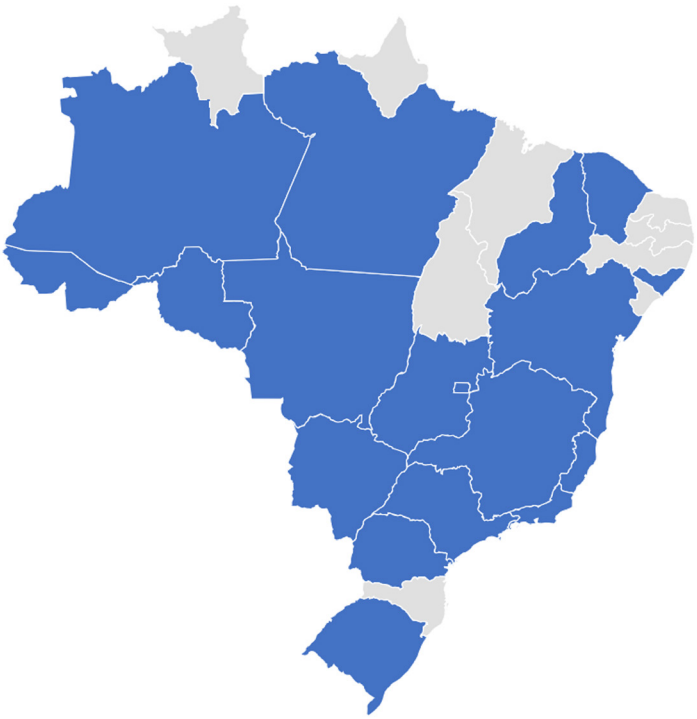

Figura 4.3 Estados brasileiros que utilizam drones.

Drones são utilizados para monitoramento de áreas de risco e georreferenciamento, filmagem e fotografia de territorialidades e pessoas suspeitas, buscas em áreas de difícil acesso como matas e comunidades urbanas, persecução durante a fuga de veículos ou mesmo captura de rotas e identificação de placas, lugares e pessoas.

Essa tecnologia, para bom uso e efetividade em sua aplicação, necessita de treinamento técnico e atendimento das normas vigentes da Agência Nacional de Aviação Civil (ANAC) para sua operação, pois é considerada uma nave não tripulada para fins legais. Em Várzea Grande, município do Mato Grosso, uma turma de quinze guardas municipais concluiu o curso de formação de piloto policial de drone no final de julho de 2022, como capacitação ofertada pela corporação. Com a nova habilidade, espera-se contribuir com operações de recuperação de veículos, furtados e roubados, localização de pessoas desaparecidas ou fugitivas e policiamento em grandes eventos.[23]

Dentre os estados que utilizam câmeras corporais, o mapeamento apenas levantou cinco estados de três regiões do Brasil. No Nordeste, Rio Grande do Norte e Bahia. No Sudeste, Minas Gerais, São Paulo e Rio de Janeiro. Já na região Sul, apenas o Rio Grande do Sul.

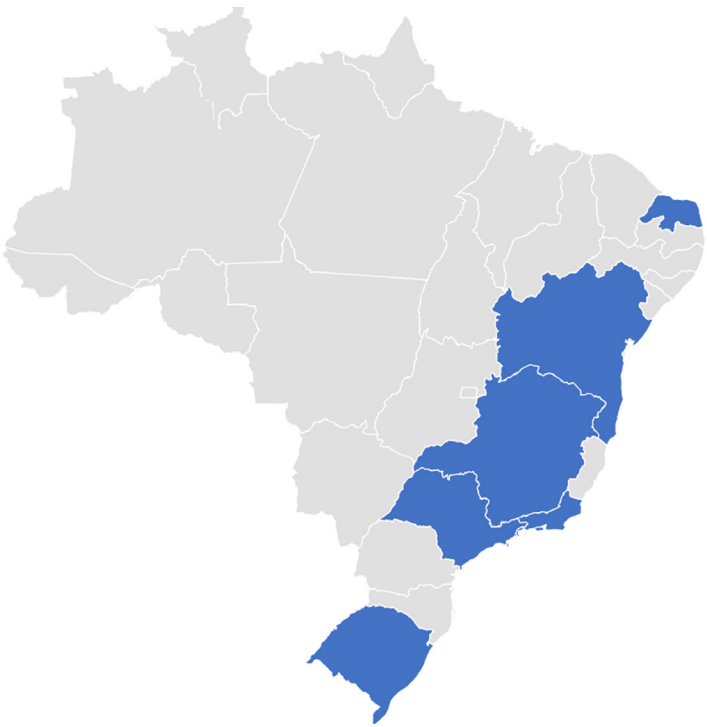

Figura 4.4 Estados brasileiros que utilizam câmeras corporais.

23 Cf. CURSO de piloto policial de drone aprimora trabalho da guarda municipal. Cuiabá: **Leiagora**, 27 jul. 2022. Disponível em: <https://www.leiagora.com.br/noticia/122938/curso-de-piloto-policial-de-drone-aprimora-trabalho-da-guarda-municipal>. Acesso em: 07 ago. 2022.

As câmeras corporais são tecnologias acopladas às fardas dos agentes de segurança, de modo que são também capazes de se integrar a outras ferramentas tecnológicas. Dentre algumas das principais promessas na adoção dessa tecnologia, destacam-se a segurança do policial, o aumento da confiança pública na polícia e a otimização do tempo de trabalho dada sua integração com outros aparatos, como sistemas interoperáveis em computadores e celulares.

A viabilidade e a necessidade do uso dessas tecnologias vêm sendo amplamente discutidos pela sociedade civil, especialmente considerando os tensionamentos entre os seus custos expressivos para os cofres públicos em confronto com as reais necessidades dos agentes de segurança, em termos de investimento em equipamentos de fato necessários em suas atividades cotidianas.

No Rio Grande do Norte, foi aprovado no primeiro semestre de 2022 um projeto-piloto da Secretaria de Estado de Segurança Pública e Defesa Social (Sesed) que prevê a instalação de quinze câmeras de monitoramento em fardas de policiais militares. O processo licitatório, finalizado em 20 de janeiro de 2022, com vitória da empresa Advanta, viabilizou fornecimento de equipamentos, treinamento de agentes e assistência técnica por três anos, após entrega dos itens.

Os custos das câmeras e softwares de gerenciamento aos cofres públicos chegaram a cerca de R$ 33.000. Santa Catarina foi o primeiro estado a adotar o equipamento no Brasil, em 2019, seguido de Rondônia e, em 2020, São Paulo, que até junho de 2021 somava mais de 2,5 mil câmeras corporais em uso em dezoito batalhões, ao custo de 1,2 milhão de reais.[24]

O mapeamento, conforme mencionado, ocorreu até 31 de maio de 2022. No entanto, é importante apresentar que em julho de 2022 a guarda municipal de Curitiba passou a contar com câmeras corporais nos uniformes das corporações e nas viaturas.

O equipamento também conta com tecnologia de reconhecimento facial para habilitação do uso, sendo estas as cinquenta primeiras câmeras que integrarão o conjunto de 515 equipamentos de alta tecnologia destinados ao uso, ao custo de R$ 791.000, a título de aquisição, manutenção e substituição de

---

24 Cf. POLICIAIS do Rio Grande do Norte terão câmeras em uniformes em 1º semestre. Natal: **Tribuna do Norte**, 23 fev. 2022. Disponível em: <http://www.tribunadonorte.com.br/noticia/policiais-do-rio-grande-do-norte-tera-o-ca-meras-em-uniformes-no-1ao-semestre/532566>. Acesso em: 07 ago. 2022.

equipamentos no que for necessário. A iniciativa faz parte do projeto "Muralha Digital", com expectativa de funcionamento integral até 30 de outubro de 2022.[25]

O Panóptico, projeto do Centro de Estudos de Segurança e Cidadania (CESeC), lançou, no dia 15 de setembro de 2022, um fascículo da estreia da Coleção Panorama dedicado ao tema das câmeras corporais. Em capítulo dedicado ao uso dessa tecnologia no Brasil, apresentou um levantamento dos estados e municípios com projetos de câmeras corporais em andamento no Brasil em quatro etapas: 1. Evidência de uso; 2. Em teste; 3. Processo de Implementação e 4. Projeto Piloto. Com destaque para os estados em processos mais avançados de implementação, como Santa Catarina e São Paulo (conforme evidenciado logo mais no subcapítulo dedicado aos aspectos comparativos entre São Paulo e Ceará).

Figura 4.5 Panorama dos estados e municípios com projetos de câmeras corporais em andamento no Brasil.

Fonte: Câmeras corporais. Lima, Nunes, Cruz (2022).

25 Cf. GUARDA Municipal de Curitiba recebe as primeiras câmeras de uniforme. Paraná: **Bem Paraná**, 11 jul. 2022. Disponível em: <https://www.bemparana.com.br/noticia/guarda-municipal-de-curitiba-recebe-as-primeiras-cameras-de-uniforme#.YvCG7OzMLR0>. Acesso em: 07 ago. 2022.

Em Santa Catarina, o projeto para uso de câmeras começou em 2018, de modo que a polícia militar do estado atualmente conta com mais de 2.000 câmeras corporais acopladas em pelo menos um policial, em cada guarnição. Já em Rondônia, somam-se 1.250 câmeras corporais utilizadas pela PM do estado, com vias para ampliação do projeto (Lima *et al*, 2022).

No que concerne ao policiamento preditivo, apenas dois estados brasileiros foram mapeados como usuários da tecnologia a partir de *web scrapping,* via declarações institucionais em veículos de grande circulação: Ceará e São Paulo. O policiamento preditivo é a aplicação de modelagem por computadores a dados criminais passados, de modo a predizer atividade criminal futura (Bachner, 2013, p. 14).

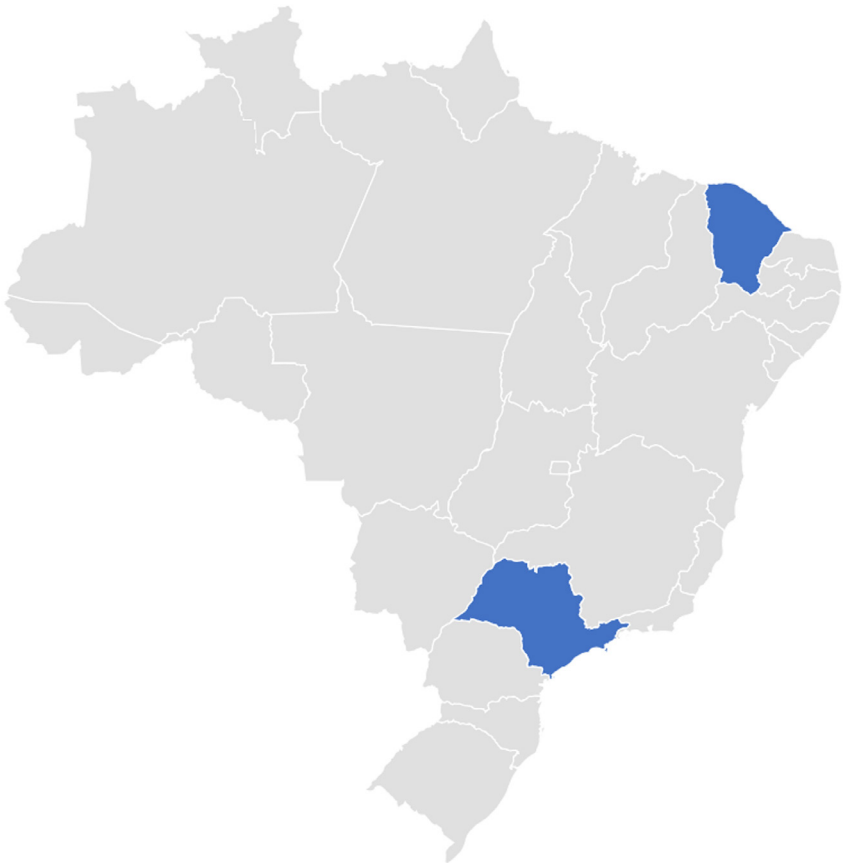

Figura 4.6 Estados brasileiros que utilizam policiamento preditivo.

Para Bachner, a noção fundamental subjacente à teoria e prática do policiamento preditivo é a possibilidade de inferências probabilísticas sobre atividades criminosas futuras com base em dados existentes. A partir da possibilidade de se utilizar dados de uma ampla variedade de fontes para calcular estimativas sobre fenômenos como onde a violência armada é susceptível de ocorrer, onde um ladrão em série é susceptível de cometer o próximo crime ou mesmo quais indivíduos um suspeito provavelmente contatará para obter ajuda.

Dados anteriores obtidos a partir de fontes convencionais e não convencionais se combinam, de modo a produzir estimativas com um grau específico de probabilidade sobre o que tenderia a acontecer no futuro. As organizações policiais, dessa forma, se utilizam desses dados para, então, tomar decisões em conformidade.

Dada a natureza direta do policiamento preditivo com o uso de dados e *analytics* de big data para a segurança pública, as regiões de São Paulo e Ceará serão submetidas a um olhar mais dedicado no subcapítulo seguinte, tanto em relação ao uso de tecnologia de policiamento preditivo quanto aos demais usos tecnológicos levantados em caráter regional.

Aspectos comparativos nos estados de São Paulo e Ceará

A cidade de São Paulo atualmente é considerada a mais populosa do país. Uma cidade de altíssima densidade populacional e desigualdade social, cujos indicadores de violência aumentaram consideravelmente em março de 2022, em comparação ao mesmo período de 2021.

De acordo com a Secretaria de Segurança Pública do Estado de São Paulo, os furtos tiveram um aumento de 52%, saltando de 33.000 para 50.467 ocorrências. Os roubos subiram 22%, saltando de 17.000 para perto de 21.000 ocorrências. Os homicídios dolosos cresceram de 237 para 241, enquanto os homicídios culposos aumentaram em 56%, saindo de dezesseis para 25 no ano passado. Além disso, o indicador de roubos de veículos teve um aumento de 36%, enquanto a quantidade de registros de carros furtados aumentou 31%. (Gonçalves, 2022).

A cidade de São Paulo apresenta muitos desafios no campo da segurança pública, e o uso de aparatos tecnológicos tem sido colocado em foco para a mitigação de muitos dos grandes desafios que a cidade apresenta. O fortalecimento

dos processos de investigação policial perpassa por modernizar as tecnologias de resposta ao crime, sobretudo no contexto de uma sociedade hiperconectada e movida a dados, com todos os desafios que isto representa.

Associando os critérios de pesquisa e a metodologia adotados no mapeamento nacional ao aspecto regional, foram identificadas as seguintes tecnologias noticiadas como utilizadas pelos órgãos de segurança do estado de São Paulo:

O reconhecimento facial foi aplicado no estado de São Paulo no ano de 2020, em fase de testes, a partir de um sistema capaz de cruzar fotos e vídeos de suspeitos em cenas de crime com o rosto de 35 milhões de pessoas em documentos de identidade emitidos pelo Instituto de Identificação Ricardo Gumbleton Daunt (IIRGD).

Figura 4.7 Tecnologias utilizadas por órgãos de segurança no estado de São Paulo.

A empresa desenvolvedora foi a Thales Gemalto, que também fornece à polícia de São Paulo, desde 2013, o seu sistema automatizado de verificação de impressões digitais. A ferramenta de reconhecimento facial foi fruto de um

contrato de licitação vencido pela empresa em 2020, sendo que ela também é responsável pelo sistema de biometria utilizado pelo governo norte-americano em aeroportos e embaixadas para controle de imigração em todo o mundo (Paiva, 2019). O recurso foi testado durante jogos da Copa América.

O recurso vem sendo alvo de críticas e de descrença por parte da sociedade civil e de entidades públicas de proteção à defesa dos direitos fundamentais. Em 2021, foi interposta uma ação em face do Metrô de SP com o objetivo de impedir a instalação em curso de câmeras de reconhecimento facial em suas instalações.

A ação foi movida pela Defensoria Pública de São Paulo, Defensoria Pública da União, Instituto Brasileiro de Defesa do Consumidor (Idec), Intervozes, Coletivo Brasil de Comunicação Social, Artigo 19 e Coletivo de Advocacia em Direitos Humanos (CADHu), segundo as quais, o sistema de reconhecimento facial teria custado mais de cinquenta milhões de reais aos cofres públicos e não atenderia aos requisitos legais previstos na Lei Geral de Proteção de Dados (LGPD), no Código de Defesa do Consumidor (CDC) e no Estatuto da Criança e do Adolescente (ECA), além de tratados internacionais e legislações setoriais.

O Tribunal de Justiça de São Paulo (TJSP) negou o recurso do Metrô e manteve a liminar de primeiro grau que proibiu a instalação imediata das câmeras, por decisão da 5ª Câmara de Direito Público (Cruz, 2022). O caso segue em disputa, ainda sem decisão transitada em julgado.

A despeito das disputas em jogo no cenário estadual, o mapeamento também apontou para o crescimento no uso de reconhecimento facial nas municipalidades do estado de São Paulo. O município de Limeira, por exemplo, localizado na região centro-oeste do estado, iniciou, em junho de 2022, um novo sistema de monitoramento que usa reconhecimento facial, a ser operado pela Guarda Civil Municipal (GCM). Ao todo, foram instaladas nove câmeras com sistema de monitoramento, capazes de identificar trinta características de pessoas e veículos.[26]

A prefeitura de Campinas, ainda em 2018, implantou tecnologia de reconhecimento facial e outras funcionalidades de segurança a partir do projeto "Cidade Segura Campinas", cujo projeto-piloto foi realizado em regime de parceria entre a

---

26 Cf. TERMINAL central de Limeira começa a usar câmeras de reconhecimento facial. Piracicaba e Região: **G1**, 10 jun. 2022. Disponível em: <https://g1.globo.com/sp/piracicaba-regiao/noticia/2022/06/10/terminal-central-de-limeira-comeca-a-usar-cameras-de-seguranca-com-reconhecimento-facial.ghtml>. Acesso em: 07 ago. 2022.

prefeitura, a empresa chinesa Huawei e o Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPQD). Em ampliação ao projeto "Campinas Bem Segura", a iniciativa teve apoio do então Ministério da Ciência, Tecnologia, Inovações e Comunicações e do Banco Interamericano de Desenvolvimento (BID). Foram instaladas trinta câmeras integradas à Central de Monitoramento (Cimcamp), com instalações majoritariamente locadas na região central da cidade.[27]

A pequena prefeitura de Aguaí, no estado de São Paulo, detém menos de quarenta mil habitantes e também inaugurou, em janeiro de 2022, uma central de monitoramento, com câmeras distribuídas em pontos estratégicos do município, dotadas do recurso de reconhecimento facial para auxiliar as atividades dos agentes de segurança pública na região.[28]

A licitação do Smart Sampa prevê a instalação de vinte mil câmeras de reconhecimento facial na cidade até o ano de 2024, o que gerou abertura de inquérito por parte do Ministério Público de São Paulo em janeiro de 2023 para averiguação de questões inconclusivas, como a ausência de informações sobre o banco de dados que será utilizado no sistema (Schendes, 2023). A prefeitura sofreu críticas e ataques após anunciar que o sistema seria capaz de monitorar e classificar pessoas como suspeitas e rastreá-las de acordo com suas características físicas, inclusive tom de pele. Apesar de suspensa a licitação até o momento, a prefeitura pretende retomar o programa, que sofrerá reanálises. (Petrocilo *et al*, 2022).

Em relação às câmeras corporais, a polícia militar de São Paulo lançou em 2021 o projeto "Olho Vivo", que trazia um sistema de câmeras corporais acopladas ao uniforme dos agentes de segurança e gravava a sua rotina de trabalho. O projeto tem se apresentado como referência no uso de câmeras corporais em todo o Brasil.

O sistema de câmeras acopladas aos uniformes grava a rotina de trabalho dos agentes de segurança, de modo que os equipamentos são instalados nas fardas dos policiais e registram não apenas vídeo em tempo real, mas áudio. Ele ganhou manchetes nos principais jornais do país devido à publicação de estudo sobre o impacto das câmeras corporais na ação policial, realizado em parceria

---

27 Cf. PREFEITURA apresenta cidade segura com câmeras de reconhecimento facial. Campinas: **Portal da Prefeitura**, 13 dez. 2018. Disponível em: <https://portal.campinas.sp.gov.br/noticia/35530>. Acesso em: 08 ago. 2022.

28 Cf. INAUGURAÇÃO da central de videomonitoramento. Aguaí: Imprensa. Noticias. **Prefeitura Municipal de Aguaí**. 07 jan. 2022. Disponível em: <https://aguai.sp.gov.br/home/28094/elementor-28094/>. Acesso em: 08 ago. 2022.

entre a polícia militar do estado, o Núcleo de Estudos da Violência (NEV), da Universidade de São Paulo, e o Centro de Ciência Aplicada à Segurança Pública (CCAS — FGV/SP). (Monteiro *et al*, 2022)

Segundo o estudo, houve uma expressiva redução: de 87% no número de confrontos e de 32,7% nas ocorrências de resistência a abordagens nos batalhões da polícia militar que adotaram o sistema de câmeras pessoais, em comparação àqueles que não os adotaram. São dez vezes menos conflito. Outros números apontaram para uma queda de 32,7% de resistências a abordagens policiais, em comparação a 2019, 2020 e 2021 (Mello, 2022).

Não tardou para o surgimento de algumas controvérsias envolvendo o uso da tecnologia, em especial o conflito entre os argumentos de potencial relação mais segura entre polícia e sociedade e a possível inibição da ação policial, com consequente aumento da criminalidade. No terceiro e quarto trimestre, registrou-se uma redução significativa no índice de letalidade nos batalhões que as adotaram, de 77,4% e 47%, respectivamente, e um aumento de 9,1% e 10,9% nos demais, que não utilizaram a tecnologia. (Lima *et al*, 2022, p. 14)

Em relação ao uso de drones, o Governo do Estado de São Paulo, através da Secretaria de Segurança Pública, iniciou em 2019 o projeto "DronePol", focado em equipar e preparar a polícia militar, civil e técnico-científica para utilizar essa ferramenta nas atividades de defesa civil e segurança pública. O projeto teve o investimento de 6,3 milhões de reais e leva em conta as características operacionais que ele oferece, de voar em ambientes hostis e confinados, sem exposição das vidas humanas, além de outros aspectos relevantes para missões de inteligência (Pedrezani, 2019).

Em 2021, o programa já contava com 33 aeronaves, que auxiliaram pela primeira vez a realização de todo o mapa de risco geológico das 32 subprefeituras da cidade, desonerando a contratação de serviços e contabilizando de maneira eficaz 489 áreas de risco. O investimento em novos equipamentos foi possível graças a um processo licitatório iniciado em 2020, cuja compra exigiu o importe de R$ 998.740, de recursos próprios da Secretaria Municipal de Segurança Urbana, mostrando-se um recurso importante para a entrega de resultados mais positivos em segurança urbana.[29]

---

29 Cf. NOVOS drones adquiridos pela secretaria de segurança urbana auxiliam na produção do mapa de risco geológico da cidade. Cidade de São Paulo. **Notícias**. Secretaria Especial de Comunicação, 17 mai. 2021. Disponível em: <https://www.capital.sp.gov.br/noticia/

Em junho de 2022, a Secretaria Municipal de Segurança Urbana certificou 44 novos pilotos de drone na Guarda Civil Metropolitana de São Paulo. Ao todo, 706 agentes de todos os órgãos públicos brasileiros já estão aptos a realizar ações de fiscalização e monitoramento com o emprego de drones no território nacional.[30]

As tecnologias de OCR têm sido um carro-chefe importante no estado e nos municípios de São Paulo para fins de modernização e monitoramento das investigações criminais. Mas os passos vêm de longe: desde 2010 foram constituídos comitês técnicos com o objetivo de viabilizar a implantação do projeto de rede de câmeras *Optical Character Recognition* no âmbito do sistema de videomonitoramento da cidade de São Paulo, viabilizado com a inicial contratação de quinhentas câmeras com software OCR pela portaria 441/11 SMSU. O objetivo foi conciliar tecnologia e inteligência aos indicadores de criminalidade e vulnerabilidade, propiciando melhores respostas por meio de investimentos em sistemas que se mostravam eficientes a partir de exemplos comparados no exterior.[31]

O videomonitoramento integrado por câmeras OCR tem como foco o monitoramento da circulação de veículos em pontos estratégicos que se mostrem relevantes para reprimir a criminalidade. O uso da tecnologia permite o monitoramento de áreas amplas, incluindo aquelas que apresentam grande fluxo de pessoas e veículos, e contribui para a identificação de veículos envolvidos em ocorrências em regiões importantes da cidade.

As câmeras OCR produzem resultados e levantamentos de informações a partir das leituras ópticas que, por sua vez, geram outros dados capazes de formar estatísticas para a análise de inteligência e o acionamento dos responsáveis pelas ações monitoradas. Isso reduz o tempo de resposta das ações preventivas e repressivas de segurança pública a todos os órgãos parceiros integrados, razão pela qual essa tecnologia é uma peça fundamental para dois elementos centrais para a modernização tecnológica da polícia: big data e integração.

A concepção de sistema integrado e avançado de inteligência e observação de indicadores há muito se mostra um projeto dos órgãos de segurança pública. Em análise a documentos oficiais, como o Projeto de Rede de Câmeras OCR, apresentado pelo Gabinete de Gestão Integrada de segurança da cidade de São Paulo em

---

novos-drones-adquiridos-pela-secretaria-de-seguranca-urbana-auxiliam-na-producao-do-mapa-de-risco-geologico-da-cidade>. Acesso em: 08 ago. 2022.

30 Idem.

31 Cf. http://legislacao.prefeitura.sp.gov.br/leis/portaria-secretaria-municipal-de-seguranca-urbana-441-de-7-de-dezembro-de-2011/consolidado.

2011, já se vislumbrava que as imagens e informações provenientes de câmeras com OCR permitiriam a cada órgão integrado promover e atuar na sua respectiva área de competência a partir de bancos de dados que serviriam às polícias e organismos parceiros (como o Detran e o Denatran, por exemplo, mas não exclusivamente). A ver:

> As polícias civil, militar e federal valer-se-ão das imagens e informações integradas para o monitoramento das ocorrências criminais, identificando os veículos irregulares e envolvidos em crimes, constantes dos bancos de dados das polícias e dos organismos parceiros, com possibilidade de visualização em tempo real dos deslocamentos decorrentes de homicídios, roubos a bancos e estabelecimentos comerciais, sequestros relâmpagos, roubos e furtos de veículos e outras ocorrências inclusive administrativas de interesse nos trechos do território da cidade de São Paulo, priorizados conforme indicadores, facilitando a atuação operacional, a identificação e prisão dos autores e de veículos, conforme o caso.

Diversas municipalidades fora da capital já detêm a tecnologia, como Fernandópolis, Santos, Piracicaba, Várzea Paulista, entre outras, de modo que o governador eleito, Tarcísio de Freitas, anunciou publicamente não prever alterações à medida que obriga o uso de câmeras corporais por policiais no Estado de São Paulo. (Cruz, 2023)

O estado do Ceará, por sua vez, tem sido considerado um dos grandes expoentes na aplicação de tecnologias para aprimoramento da segurança pública no país. Dentre as tecnologias perquiridas neste mapeamento regional, foram identificadas:

Figura 4.8 Tecnologias utilizadas por órgãos de segurança no estado do Ceará.

A Secretaria de Segurança Pública e Defesa Social (SSPDS) do Ceará recebeu o *Prêmio Latin Trade Citizen Security*, concedido pela *Revista Latin Trade* em 2021 na categoria "uso de ferramentas analíticas de combate ao crime", em cerimônia realizada em Nova York.[32]

A tecnologia desenvolvida pelo estado apresenta diferencial a partir da criação da Superintendência de Pesquisa e Estratégia de Segurança Pública (Susesp), um setor dedicado ao desenvolvimento de tecnologia de ponta e pesquisas científicas com o objetivo de solucionar problemas do dia a dia.

O Agílis é um exemplo, pois o sistema é uma plataforma que conta com mapas, imagens e demais informações, capaz de integrar diversos bancos de dados de modo a ajudar na identificação de veículos utilizados em crimes ou relacionados a pessoas em conflito com a lei. O Agílis é um sistema de inteligência artificial que, aplicado ao Núcleo de Videomonitoramento (Nuvid) da SSPDS, passa a integrar 3.300 câmeras em cruzamento a vários bancos de dados, permitindo a identificação de veículos roubados ou usados em ações criminosas (Barbosa, 2022).

De acordo com dados da SSPDS, o estado do Ceará reduziu, entre janeiro e setembro de 2021, o índice de furtos e roubos de veículos em 10%, comparado ao mesmo período do ano anterior (Barbosa, 2022). Outra ferramenta interessante é o Sistema Tecnológico para Acompanhamento de Unidades de Segurança (Status), capaz de aplicar ciência de dados, estatística e geoprocessamento para determinar o dia da semana e horário em que determinado crime tem maior incidência. A essa aplicação, dá-se o nome de "mancha criminal".

Um expressivo exemplo de como a temática do reconhecimento facial tem passado por disputas políticas no estado é o projeto de lei para instalação de câmeras de segurança nas ruas de Fortaleza, que ingressou em regime de urgência na Câmara Municipal em outubro de 2022. Após quatorze propostas de emendas e debates travados nas comissões temáticas, treze foram rejeitadas

Dentre elas, a emenda que autorizava a instalação de tecnologia de reconhecimento facial no maquinário e a instalação de câmeras no fardamento dos guardas municipais.

---

32 https://www.sspds.ce.gov.br/tag/latin-trade/. Acesso em: 10 maio 2023.

A única emenda aprovada estabelecia que o videomonitoramento poderá atuar em interoperação com outros equipamentos públicos que já possuem câmeras instaladas (Fonseca, 2022). Porém, o cenário político ainda é instável, de modo que recentes declarações do governador eleito em 2023, Elmano de Freitas (Bandeira, 2022) e do secretário de segurança pública do Ceará, Samuel Elânio têm se inclinado no sentido da implementação das câmeras de reconhecimento facial.

Até o momento, apenas os policiais penais utilizarão câmeras em suas fardas. A partir de fevereiro de 2023, serão utilizados trezentos aparelhos na modalidade de teste, a serem distribuídos em todas as unidades prisionais.

Cidade do Rio de Janeiro: um estudo de caso

No início de 2022, foi anunciada pelo Governo do Estado a instalação de câmeras nos uniformes de policiais militares, a fim de buscar fiscalizar a atuação dos agentes. A medida faz parte do Programa Estadual de Transparência em Ações de Segurança Pública e Defesa Civil e já possuía lei anterior similar, promulgada há doze anos, que obrigava o uso de câmeras em viaturas policiais. Entretanto, tal demanda não estava sendo executada conforme o previsto.

O ampliamento de ferramentas de monitoramento também foi divulgado pela prefeitura da cidade do Rio de Janeiro, que almejou, em junho de 2021, a utilização de mais dez mil novas câmeras na cidade, sendo 40% delas com dispositivo de reconhecimento facial, mediante a expansão do Centro de Operações Rio.

Contudo, a implementação de ferramentas tecnológicas que buscam expandir o monitoramento no estado e seus agentes não é uma novidade. Desde o ano de 2007, tendo em vista a realização de megaeventos esportivos — Jogos Panamericanos, em 2007, Copa do Mundo Fifa, em 2014, e as Olímpiadas, em 2016 —, o Rio de Janeiro passou a delinear planos no âmbito da segurança pública a fim de melhor produzir tais eventos.

A “modernização tecnológica” planejada e investida pelo estado associa-se a um legado de infraestrutura a ser deixado no país, ainda que custosa, de modo que:

> O sistema de videovigilância do Rio de Janeiro, por exemplo, é apresentado como um legado dos Jogos Panamericanos de 2007 — e, mesmo se sua construção foi iniciada de forma independente, dificilmente teria se expandido com a mesma velocidade entre os anos de 2006 e 2007 sem os vultosos recursos recebidos da Secretaria Nacional de Segurança Pública (Senasp), cujo intuito declarado era promover maior segurança para a cidade durante a competição internacional que ocorreria. No caso dos megaeventos vindouros, os investimentos e estratégias vêm sendo planejados com antecedência e nível de detalhes bastante superior ao que foi visto no Pan de 2007, principalmente por terem alcance, importância e visibilidade muito mais significativas (Cardoso, 2013, p. 123).

O autor ainda complementa:

> A noção de "legado", aquilo que é deixado, que fica, permanece, tem centralidade em praticamente todos os discursos acerca dos megaeventos. Fala-se de legado em urbanismo, em obras de infraestrutura e de transportes, em estádios e instalações esportivas, e também em segurança pública. O termo é usado sem grande debate ou desacordo por praticamente todos os envolvidos com os eventos, desde as entidades privadas promotoras até os manifestantes contrários à sua realização (Cardoso, 2013, p. 126).

Em relação às tecnologias implementadas à época, a integração foi buscada como forma de melhor execução do planejado, com a criação do CICC e a união de forças da segurança pública em espaços próximos (Cardoso, 2013). Nele, "o planejamento e a execução das operações tiveram como base o que se convencionou chamar de sistema integrado de comando e controle, que acabou servindo de matriz para a política de segurança que foi adotada nacionalmente" (Cardoso, 2019).

O modelo de "comando e controle", adotado desde os Jogos Olímpicos de Atenas de 2004, passou a se apresentar como o que seria a principal solução para cuidar de problemas relativos a grandes eventos, em que há um aumento de despesas com segurança, e empresas e indústria de segurança viram um ponto central (Cardoso, 2019, p. 56).

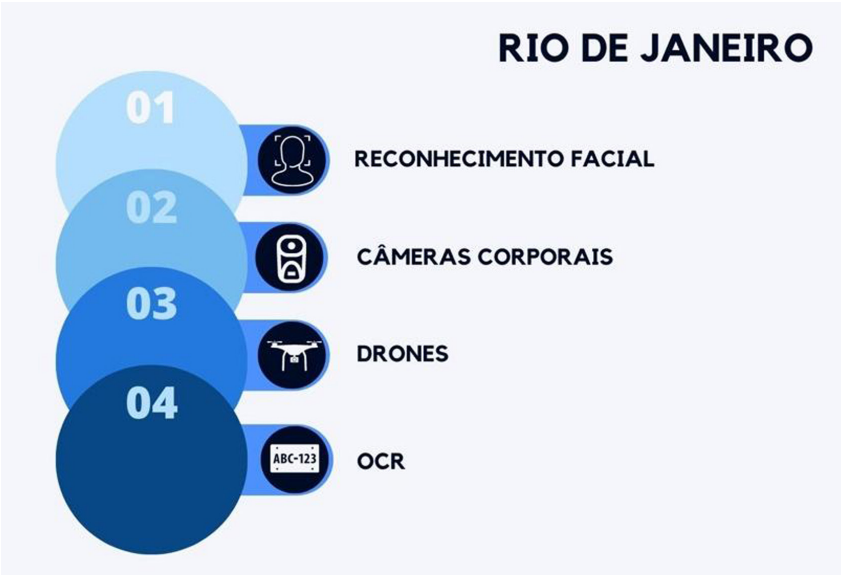

Figura 4.9 Tecnologias utilizadas por órgãos de segurança no estado do Rio de Janeiro.

O sistema de reconhecimento facial foi introduzido pela primeira vez pela Prefeitura do Rio de Janeiro em 2019, para policiamento nas festividades de Carnaval. O sistema foi anunciado com empolgação, até que, nas primeiras semanas, uma pessoa inocente foi presa indevidamente com o uso do sistema (Dias e Hvistendahl, 2021). Após denúncias da comunidade acadêmica e científica, política e de ativistas, relativas a inconsistências no sistema e riscos a direitos fundamentais, houve sua descontinuidade pela polícia para fins de maior amadurecimento para retomada da sua implementação em outro momento.

O ano de 2019 foi marcado por investimentos robustos em segurança pública no Rio de Janeiro. Houve, no período, uma liberação de quinze milhões de reais pela Assembleia Legislativa (Alerj) para investimentos em inteligência policial. O governador do Rio de Janeiro, Cláudio Castro, obteve desconcentração da verba em 2021, de maneira a somar a quantia aos investimentos robustos na construção de um novo Centro Integrado de Comando e Controle na Baixada Fluminense (CICC-BF). A iniciativa teve valor estimado de investimento inicial de 31 milhões de reais e foi inaugurada em julho de 2022.

O Centro oferece recursos tecnológicos de última geração que estão em processo de testes no equipamento, com cerca de trezentas câmeras fixas e móveis

já instaladas pela cidade para monitoramento de vias públicas, no intuito de auxiliar as ações de segurança pública na cidade.[33] Mais uma vez, o escopo de integração reaparece e ganha concretude nesta iniciativa, ao que a prefeitura alega que irá receber a base de dados do Ministério da Justiça e, com isso, tornar o CICC-BF integrado à rede nacional de dados, permitindo a agilização e a racionalização de medidas operacionais conjuntas entre diversos órgãos.

Outro investimento que ganhou robustez no estado foram os drones. Desde 2017, a polícia militar criou o núcleo de aeronaves remotamente pilotadas (NuARP), que, além de ter priorizado pesquisas para a aquisição de equipamentos de alta qualidade, recebeu, em 2018, dois sistemas remotamente pilotados do Gabinete de Intervenção Federal (GIF), realizando treinamentos de habilitação para que policiais pudessem manusear a tecnologia.[34]

No ano de 2022, o Governo do Estado adquiriu 35 drones de última geração para serem utilizados na área de segurança pública em operações policiais, vistorias em presídios e em apoio a fiscalizações ambientais. O equipamento foi adquirido em pregão eletrônico em 17 de agosto de 2022, por R$ 95.305.074,57 (Goes, 2022). O equipamento foi utilizado no Réveillon do mesmo ano. (Alves, 2022)

Por outro lado, o jornal *The Intercept Brasil* noticiou a suspeita de compra de um enorme pacote de serviços de infraestrutura da multinacional *Oracle* com softwares capazes de fazer cruzamentos e análises de grandes volumes de dados. Dentre as muitas promessas da tecnologia oferecida às autoridades policiais do Rio de Janeiro, destaca-se o policiamento preditivo.

A reportagem de março de 2021 realizou pedidos via Lei de Acesso à Informação (LAI) à polícia civil do Rio de Janeiro, que respondeu não haver nenhum contrato vigente com a empresa *Oracle*. No entanto, ao promoverem uma busca no portal da transparência, havia três contratos ativos relativos à manutenção de software e bancos de dados fornecidos pela empresa, de modo que a área de combate e prevenção a crimes, sozinha, foi responsável pelo gasto de quinhentos mil reais em 2020 pelos serviços prestados (Dias e Hvistendahl, 2021).

---

33 Cf. CLÁUDIO CASTRO visita obras estruturantes em Duque de Caxias. **Jornal O Dia**, 14 mai. 2022. Disponível em: <https://odia.ig.com.br/duque-de-caxias/2022/05/6401298-claudio-castro-visita-obras-estruturantes-em-duque-de-caxias.html>. Acesso em: 26 jan. 2023.

34 Cf. PMERJ intensifica uso de drones em operações de segurança pública. Rio de Janeiro: **Piloto policial**, 02 out 2020. Disponível em: <https://www.pilotopolicial.com.br/pmerj-intensifica-uso-de-drones-em-operacoes-de-seguranca-publica/>. Acesso em: 26 jan. 2023.

O Rio de Janeiro também enfrenta um tensionamento político no que diz respeito à adoção de câmeras corporais por policiais. Apesar de já serem utilizados os equipamentos em batalhões comuns desde maio de 2022, as polícias têm se posicionado contra o seu uso em agentes de forças especiais: o Batalhão de Operações Especiais da Polícia Militar (Bope) e a Coordenadoria de Recursos Especiais da Polícia Civil (Core).

Em dezembro de 2022, foram enviados ofícios ao STF no sentido de existirem fatores que podem comprometer o êxito das operações e colocar em risco a vida dos próprios agentes (Sestrem, 2023). Sobre isso, o próprio governador do estado, Cláudio Castro, já se manifestou, na posse de seu novo mandato, contrariamente ao equipamento, afirmando que recorreria "até o fim" contra a instalação em fardas de ambas as instituições (Bandeira, 2022).

5

A adoção de novas tecnologias sob o olhar dos agentes de segurança pública no Rio de Janeiro

Metodologia e trabalho de campo

Antes de nos dedicarmos à análise propriamente dita do material das entrevistas, é importante explicitar o contexto em que foram realizadas e fornecer aos leitores os dados metodológicos que orientaram nossas análises e escolhas da pesquisa. Durante o tempo de duração deste projeto, realizamos vinte e três entrevistas com profissionais do sistema penal, englobando instituições estaduais, municipais e federais na cidade do Rio de Janeiro. A maior parte das entrevistas foi conduzida por um pesquisador acompanhado de um estagiário e o entrevistado. Em algumas delas, no entanto, mais de um entrevistado esteve presente, bem como, em alguns momentos, mais de dois entrevistadores conduziram a entrevista.

Tivemos por hábito, portanto, que dois pesquisadores, quase sempre um pesquisador e um estagiário, acompanhassem a entrevista, havendo momentos em que um deles poderia atuar mais como observador da cena. Assim, o pesquisador era responsável por conduzir as perguntas enquanto o estagiário poderia realizar a atividade de observação das reações e do cenário ao longo da entrevista.

É importante explicar que fizemos entrevistas presenciais em que nós, os pesquisadores, nos dirigimos até onde se encontravam os entrevistados, mas que também foram realizadas entrevistas por via online. É claro que, em termos metodológicos, as duas formas de interação, a face a face e a online, não são equivalentes, o que demanda que adaptações sejam feitas em entrevistas online, como a redução do tempo para evitar o cansaço do entrevistado diante da tela, a postura do entrevistador, que precisa se mostrar mais presente pela fala na entrevista por videoconferência, entre outros aspectos. Contudo, em nossa pesquisa, a entrevista online se mostrou útil quando o entrevistado não estava disponível presencialmente para realizá-la e foi utilizada como recurso subsidiário à entrevista presencial, escolhida por nós como principal via de interação com os atores pesquisados.

Dito isso, nossa proposta neste capítulo é apresentar uma análise comparativa dos diversos discursos dos profissionais que atuam nos campos do direito e da segurança, no que diz respeito ao uso da tecnologia na área da segurança pública. Por segurança pública, compreendemos não apenas as instituições de policiamento, a polícia militar e a polícia civil, mas também as instituições de justiça, o que nos levou a entrevistar promotores de justiça do estado do Rio de Janeiro e um procurador da república, como também um funcionário

da Secretaria de Ordem Pública do Município do Rio de Janeiro (SEOP) e do Instituto de Segurança Pública (ISP).

Trata-se, portanto, de análise qualitativa dos dados em que pretendemos compreender as categorias discursivas dos atores, por meio de um estudo exploratório, cujo objetivo é mapear os elementos mais relevantes associados ao tema da utilização de tecnologias na área de segurança pública, a partir da percepção dos atores entrevistados.

É importante, então, pontuarmos o nosso passo a passo de pesquisa para explicitarmos o percurso e as escolhas metodológicas que fizemos ao longo deste projeto. Isso permite pensar e problematizar nossos resultados, mas também nossas limitações, diante dos desafios que encontramos no desenvolvimento da pesquisa.

Pesquisa empírica: uma abordagem interdisciplinar

É importante destacar, primeiramente, que, neste projeto, nos alinhamos aos estudos de pesquisa empírica do campo jurídico, uma vez que nos propomos a estudar o direito a partir das práticas sociais. Compreender o direito enquanto um sistema de práticas significa analisá-lo pela forma como ele se desenvolve empiricamente, a partir das relações sociais que seus operadores, os jurisdicionados e as instituições judiciárias, produzem com os textos normativos e entre si. Trata-se de entender que o direito se produz e se reproduz nessas relações.

Isso permite que questões até então alheias à teoria do direito sejam abordadas e compreendidas como objetos de estudo que auxiliam na compreensão do campo jurídico. Dessa forma, a interdisciplinaridade, principalmente na relação entre as ciências sociais com o direito, atua no sentido de tornar inteligível a normatividade do campo jurídico e as condições sociais em que ela se apresenta. Logo, consideramos o direito enquanto objeto de estudo, e não somente como constitutivo de nossa orientação teórica.

Assim, ao considerá-lo em sua dimensão prática, o compreendemos enquanto fenômeno que pode ser descrito e analisado, premissas que transformam em exigência lógica a pesquisa empírica. Fernando Fontainha e Pedro Heitor Barros Geraldo (2015), nesse sentido, destacam que "[...] para se entender o direito de uma sociedade, devemos observar como ele se produz nas relações sociais e nos contextos institucionais, e não ler o que os livros dizem o que ele é" (Geraldo e Fontainha, 2015, p. 11).Reside nesse fato a crítica de Kant de

Lima e Lupetti Batista (2014) de que a leitura aos manuais de direito não permite compreender a lógica do sistema judiciário brasileiro e, tampouco, construir uma percepção adequada do campo jurídico.

Para Kant e Lupetti (2014), o método antropológico do trabalho de campo pode ser utilizado como uma importante via de contribuição a uma análise que apresenta outra perspectiva do direito que não aquela restrita ao seu próprio universo dogmático, ao identificar e analisar os domínios das representações e práticas jurídicas e desnaturalizar seus discursos e saberes, entendendo-os como resultantes de processos culturais, políticos e econômicos.

Essa articulação com o trabalho etnográfico extrapola os limites judiciários para abranger a problematização e análise dos conflitos sociais, a fim de saber quais significados comportam, o que representam no convívio social, como os sujeitos percebem e vivenciam seus direitos e deveres, orientando-os para a resolução ou não desses conflitos. Com isso, apresentam-se novos temas e problemas que são marginalizados ao debate acadêmico jurídico clássico.

Neste trabalho, não nos propomos a fazer uma etnografia nem a utilizar métodos antropológicos de pesquisa. Numa abordagem mais próxima das ciências sociais, poderíamos dizer que nos apropriamos de um olhar sociológico para o nosso objeto de pesquisa, e que utilizamos de técnicas sociológicas de coleta e análise de nossos dados, uma vez que a sociologia nos oferece mais recursos metodológicos de análise e produção de dados empíricos. Isso para, nos termos de Geraldo e Fontainha (2015), compreendermos o direito em ação, na medida em que as técnicas e teorias sociais são tomadas como meio para analisar o direito enquanto fenômeno.

Diante disso, optamos por realizar entrevistas semiestruturadas com duração de cerca de uma hora por entrevistado, variando um pouco para menos ou para mais tempo, mas nunca nos afastando muito desta margem. Consideramos um tempo razoável para que o entrevistado pudesse falar com tranquilidade sobre as temáticas e um bom tempo para conseguirmos negociar as entrevistas no cotidiano atarefado destes profissionais.

Não definimos, a priori, um número fechado de entrevistas nem quem seriam os entrevistados. O campo foi se abrindo conforme avançávamos nas conversas com os atores pesquisados. Uma entrevista, por vezes, abriu caminho para muitas outras, com um ator indicando os próximos entrevistados e

nos mediando esses contatos, ao mesmo tempo que pode ter nos desligado de outras possibilidades.

Assinalamos aqui que nossas entrevistas não são lidas nem analisadas por nós como amostragem quantitativa. O que propomos é uma leitura qualitativa que busque compreender os sentidos das práticas e dos discursos no campo da segurança pública, a partir das perspectivas dos próprios profissionais, o que nos fez optar por entrevistas aprofundadas com cada um desses atores, em uma interação que nos permitisse compreender os pontos de vista de cada um dos entrevistados.

As entrevistas na prática: negociações e recusas

Em algumas instituições, tivemos mais facilidade de contato, como na polícia militar e no Ministério Público Estadual, motivo pelo qual conseguimos realizar mais entrevistas. Em contraposição, o acesso à polícia civil encontrou muitos entraves. Realizamos diversas tentativas de visitas à Cidade da Polícia (CIDPOL), espaço institucional da polícia civil que conta com diversas delegacias especializadas e com órgãos de chefia desta instituição

Nos momentos em que estivemos na CIDPOL, os delegados se negaram a nos dar entrevistas ou marcavam outros momentos para voltarmos, mas não nos concederam entrevistas. Além disso, também tentamos contatos, em paralelo, diretamente com delegados que conhecíamos, buscando ativar a rede de relações dos pesquisadores.

Aparentemente, a própria escolha do tema de pesquisa, objeto de conversa nas entrevistas, gerava a preocupação dos entrevistados com o que poderia ou não nos ser revelado. De maneira geral, essa preocupação dos atores com a publicização de algumas informações nos acompanhou durante toda a pesquisa. Uma das entrevistas inclusive foi acompanhada por um funcionário que trabalhava na área de comunicação da instituição e que estava ali responsável por acompanhar o que estava sendo dito, para garantir que nenhuma informação confidencial fosse mencionada durante a entrevista.

Assim, em muitos contatos anteriores às entrevistas, nos momentos em que negociávamos agendamentos e autorizações, a preocupação com a publicização de temas considerados confidenciais pelos entrevistados foi levantada como uma carta para modular as questões dos pesquisadores, para negociar temas abordados e até mesmo como justificativa para negar entrevistas. Este foi

um problema com o qual tivemos que lidar, enquanto grupo de pesquisa, desde o início de nosso projeto.

Diante de uma lógica da desconfiança que se manifesta por uma burocracia cartorial, não é de se estranhar que os ambientes policial e do sistema de produção judicial não sejam campos de entrada fácil para os pesquisadores. Vistos como aqueles que produzirão um olhar externo da instituição, eles podem ser interpretados como ameaças para produzir fiscalização ou controle da atividade desses profissionais.

Nesse aspecto, vale ressaltar que os comportamentos da polícia civil e militar diferiram de maneira acentuada em nossa pesquisa. Talvez, em parte, também pelos nossos contatos e o que poderíamos chamar de informantes, que nos auxiliaram a conseguir as entrevistas, tivemos uma entrada muito receptiva na polícia militar, com direito a tour por prédios responsáveis pela área mais tecnológica desta polícia e fotos para registrar os encontros com os oficiais, ao contrário da polícia civil, que se fechou institucionalmente diante das nossas investidas. Por outro lado, essa diferença de reação pode se identificar com a própria distinção de atividade relativa a cada uma dessas polícias: a polícia civil se relaciona à atividade mais discreta de investigação e inteligência da persecução penal, enquanto a polícia militar é responsável pelo policiamento ostensivo.

Entrevistas

As entrevistas foram gravadas e desidentificadas para preservar o anonimato de nomes, lugares e pessoas. O objetivo foi que os entrevistados descrevessem suas práticas, aquilo que eles fazem ou fizeram em suas atividades corriqueiras de trabalho, numa tentativa de situar as entrevistas no centro das práticas sociais.

Optamos por comparar os discursos de atores de diferentes instituições, traçando um paralelo entre as lógicas e compreensões do que é a atividade de segurança para cada um desses atores. Importante esclarecer que as falas dos interlocutores aparecerão destacadas como citação quando tiverem mais de quatro linhas, e no corpo do texto, entre aspas e em itálico para demarcar a fala nativa.

Suprimimos nomes pessoais ou a menção a títulos e cargos para desidentificar os atores, optamos por chamá-los aqui com o nome da instituição a que pertencem, por exemplo “promotor de justiça” ou “policial militar”, entre outras nomenclaturas que poderão ser observadas no texto. Ressaltamos que as

marcas de oralidade presentes nos discursos foram mantidas, de modo que o leitor deste trabalho encontrará as falas transcritas com a maior fidelidade possível ao discurso real dos interlocutores.

Adoção de aparatos tecnológicos sob o olhar dos agentes de segurança pública no Rio de Janeiro

"Comprar computador não é ter tecnologia, isso aí é uma máquina de escrever moderna": considerações sobre o conceito de tecnologia

Conforme mencionado em capítulo anterior, a relação da tecnologia com o campo da segurança pública na cidade do Rio de Janeiro foi transformada de forma intensa devido ao fato de a cidade ter sediado grandes eventos, como a Copa do Mundo de 2014 e as Olimpíadas de 2016. Bruno Cardoso (2019) explica que o modelo gerencial-militar de segurança pública foi reforçado como forma principal de planejamento, conforme tópico abordado em capítulo anterior deste relatório. Os entrevistados que integram quadros da polícia militar, da mesma forma, destacaram o impacto dos grandes eventos na utilização de tecnologias:

> Na corporação, a gente está evoluindo para um cenário em que a TI vai ter mais relevância, eu acho. Melhorou muito. Hoje já se entende… (Policial Militar 4).

> Hoje parece que deu um *boom*. Alguém entendeu, esse botão virou, de uns quatro anos pra cá, de uma forma que eu achei que ia demorar mais. A gente cresceu muito em quatro anos (Policial Militar 5).

> E os grandes eventos foram fundamentais para acelerar esse processo… pegando gancho na pergunta sobre integração, o governo do estado, com o pessoal da secretaria de transporte, mais o Comandante Geral, achou por bem unir esforços, unir tecnologias, unir o contato, o conhecimento e as experiências (Policial Militar 2).

Vale destacar neste ponto que os atores durante as entrevistas pontuaram em diversos momentos o que compreendiam por tecnologia e o que não seria assim reconhecido dentro de suas concepções. O Policial Militar 1, por exemplo, explica que;

> O que você tem é compra: "Ah, comprar computador". *Comprar computador não é ter tecnologia, isso aí é uma máquina de escrever moderna*

> *e o que eu quero é métodos, metodologias que eu possa analisar dados né, cristalizar informações, fazer análises e eu, tomador de decisão, possa decidir com os melhores números, né* (Policial Militar 1, grifo nosso).

Comentário bem parecido foi feito pelo Promotor de Justiça 1:

> *Por isso na minha opinião, ainda estamos no sistema de informática departamental, porque foi assim que começou. Ah, agora tem computador, né? O que isso significa? É a nova máquina de escrever. Tira a máquina de escrever e coloca o computador. Pronto, agora tem tecnologia. Não, não é!* Isso se reflete, por exemplo, na formação das perícias de polícia. Eu estava examinando, essa semana, o conteúdo programático no curso da Acadepol de formação de peritos forenses digitais. É claramente um modelo focado na apreensão de hardware, que é o que predominava dez anos atrás. Ninguém está ali pensando primeiro em forense digital mobile, em forense de memória, em forense de rede, em forense de nuvem, ou seja, tem sempre esse descasamento entre o que a gente está fazendo, o que a gente está ensinando e o que está acontecendo, que é um fenômeno jurídico, de qualquer forma, como isso acontece cada vez mais rápido, esse distanciamento, na minha opinião, está ficando cada vez maior (Promotor de Justiça 1, grifo nosso).

A perspectiva de que a tecnologia deva ser utilizada para medir e classificar também surgiu na fala do Policial Militar 3:

> Pesquisadora: O senhor comentou também que teve, um pouco, uma mudança, né, nesse uso da tecnologia, cada vez mais para um foco gerencial… Policial Militar 3: É, mais interessado em medição, em mensuração, né. É aquela frase do William Deming, "o que não pode ser medido, não pode ser gerenciado". Então a gente leva isso daí, acho que desde 2008, 2007 que é, foi instituído esse *sistema de metas*, que é a frase que mais representa esse trabalho, entendeu? *Porque se você não conse… não mede, você não gerencia, entendeu? Então é o que norteava esse trabalho.* (Policial Militar 3, grifo nosso).

O sistema de metas a que se refere o Policial Militar 3 foi explicado em entrevista com uma interlocutora que trabalha no ISP, autarquia estadual vinculada à Secretaria de Planejamento do estado do Rio de Janeiro. Ela explica que:

> O Sistema Integrado de Metas é o programa de segurança pública mais antigo do nosso estado. Ele foi criado pela então Secretaria de Segurança, né? E com a extinção da Secretaria de Segurança, como eu havia mencionado, em 2018, ele passou a gestão para o Instituto de Segurança Pública. Muito resumidamente, a gente tem vários e vários manuais e legislações para falar do SIM, como ele é conhecido, Sistema Integrado de Metas. *Ele é um programa de gestão que teve como objetivo introduzir uma cultura de gestão para as polícias com base em análise criminal*. Para isso, ela tem uma série de premissas, dentre as quais, a principal é a integração entre as polícias, né. Tem uma série de reuniões, entre as polícias civil e militar, porque entendeu-se que com a integração era menos difícil chegar às metas de redução de criminalidade. Ela também coloca metas de redução para os indicadores estratégicos. Então, a Cúpula de Segurança Pública do nosso estado se reúne e traçam estratégias para a segurança pública, quais são os indicadores criminais, onde que as polícias precisam mais atuar, quais são os crimes que são mais estratégicos, digamos assim, para a segurança pública, e coloca metas de redução semestralmente. Para isso, tem as reuniões de nível em que a Cúpula conversa e, também, temos a premiação para aquelas regiões que conseguirem alcançar meta. Então, toda a gestão desse programa fica aqui no Sistema de Gestão de Metas do ISP. O ISP é responsável por essa gestão (Interlocutora ISP, grifo nosso).

Assim, percebemos que a tecnologia não é definida pelos discursos de nossos interlocutores simplesmente como as ferramentas utilizadas. Eles não falam apenas de computadores ou softwares ou outros equipamentos, o que fica claro até pelos discursos dos atores ao mencionarem expressamente "do que não estão falando" quando se propõe a pensar sobre tecnologia.

Como entrevistamos agentes que ocupam cargos de gestão da polícia militar, delegados da polícia civil e promotores do Ministério Público, podemos problematizar que talvez esses atores tenham uma visão mais geral das instituições em que trabalham e dos papéis dessas instituições dentro do funcionamento do sistema de justiça criminal.

Para as entrevistas, também nos foram indicados interlocutores que trabalhavam próximo ao desenvolvimento de tecnologias ou em setores/departamentos dessas instituições responsáveis pela utilização mais direta das ferramentas tecnológicas. Isso nos leva a ressaltar o alto grau de reflexividade dos atores

entrevistados. Assim, tivemos entrevistas marcadas por falas que destacaram críticas e descreveram processos político-históricos dentro das instituições.

Nesse sentido, os atores entrevistados parecem se preocupar não apenas com a tecnologia em si, em um sentido puro, da ferramenta tecnológica, mas com os arranjos burocráticos e institucionais responsáveis por tornar a tecnologia efetiva aos fins almejados.

É nesse contexto que o Policial Militar 3, ao descrever o teste com a tecnologia de reconhecimento facial que foi realizado em 2019 no bairro de Copacabana, nos explica os resultados alcançados, as falhas e a repercussão do teste posteriormente. Assim, ele nos abre a sua conclusão sobre os diversos questionamentos que foram feitos à polícia militar diante dessa ocasião.

Reproduzimos uma fala longa, mas que demonstra a reflexividade dos nossos atores, além de explicitar como eles ouviram a crítica que veio da Anistia Internacional e como tentaram respondê-la internamente, pois a conclusão final foi de não adoção da tecnologia de reconhecimento facial:

> Aí a gente falou, "olha, isso tá dando problema, tem tanto questionamento sobre o uso, a Anistia Internacional, o Fórum de Segurança Pública, tanta gente mandando tanto questionamento sobre o uso disso aí. Vamos esperar a poeira baixar, esperar assim, esperar a não… não é nem a poeira baixar, mas é, vamos esperar a maturidade das pessoas e do próprio sistema. *Aí foi quando eu falei da necessidade de uma legislação que colocasse certos limites no uso judicial da ferramenta*, porque essa tecnologia é muito bacana, muito bacana, muito interessante. *Mas uma pergunta que eu achei complicada, até de responder, foi de uma representante da Anistia Internacional. Que ela falou, "ah, mas e se alguém quiser utilizar isso daí pra perseguir os seus opositores?"*. Eu falei, "olha", respondi pra ela, "olha, é… não é o escopo do nosso projeto, sabe. Tanto, a gente não pegou na construção da base de dados. A gente já partiu de uma base de dados conhecida, de mandados de prisão, que está pública inclusive, né. No banco de dados nacional, o Banco Nacional de Mandados de Prisão, o BNMP". Tá lá, lá do CNJ (Conselho Nacional de Justiça). A gente pegou isso, contrastou, você vai ver, tá tudo lá. Agora, é, inclusive, o próprio cidadão pode ter acesso a isso, tem o SINESP Cidadão. Se a pessoa quiser saber se alguém tem mandado de prisão, é só consultar ali. O SINESP Cidadão busca nessa mesma base. E essa base…

> Pesquisadora: Mandado público, né?
>
> Policial Militar 3: É público. Essa mesma base foi utilizada pra é, parametrizar isso aqui. Então a gente não tá pegando aqui todos os cidadãos. É lógico que a gente tem um número muito grande. Só de mandado de prisão no Brasil, a gente tem mais de 380 mil mandados de prisão. Imagina se fosse cumprir tudo isso, né… não ia ter lugar pra botar tanta gente, né. Mas dentro do estado do Rio de Janeiro tem 43 mil abertos; mandados de prisão em aberto. Então assim; é muita gente para… com mandado de prisão em aberto, entendeu? *Então assim, eu respondi para ela, "olha, não é o objetivo. A gente tem aqui, o que está sendo colocado nessa base de dados, é isso. Outras pessoas não se chamam no alerta. Não alerta porque o fulaninho tá ali com uma bandeira do PT ou da CUT, ou de qualquer outra coisa, entendeu? Que se oponha ao governo, ou qualquer opositor do governo, não vai fazer isso. O sistema não está ali para isso, entendeu? O sistema é pra um benefício comum do cidadão. A ideia era essa"* (Policial Militar 3, grifo nosso).

Essa fala demonstra como o Policial Militar 3, mesmo favorável à tecnologia do reconhecimento facial, se sentiu questionado diante do uso da tecnologia, demonstrando a consciência de que a ferramenta por si só pode ter usos políticos distintos. Nesse episódio narrado por ele, a preocupação da Anistia Internacional não é supérflua, nem deve ser desconsiderada. Ele se defende da possível crítica explicitando, no caso em questão, que a tecnologia não teria sido utilizada para perseguir grupos políticos, mas não há a garantia que essa espécie de controle não possa ser realizada. Por isso ele demarca como uma questão "complicada de responder".

O Policial Militar 7 também faz uma observação que caminha nesse mesmo sentido ao destacar a importância do que ele nomeia como "governança" para utilização da tecnologia no campo da segurança pública:

> […] Mas acho que tem que se ter esse cuidado e o acompanhamento constante, daí eu vou…, só um complemento, a esse terceiro ponto. A importância da governança. Não dá para botar alguma coisa solta, envolvendo várias partes e não ter uma governança muito bem esclarecida, envolvida e que faça a coisa acontecer, soltar muito o freio de mão para o carro descer na rodadeira e achar que o carro não vai bater no muro, porque vai bater. Acho assim, enfim, é um curioso que está tentando contribuir aí para o trabalho de vocês. (Policial Militar 7).

Portanto, a forma dos interlocutores pensarem essa problemática é justamente propondo uma saída legal: a de que caberia ao Estado Brasileiro, por meio de uma regulamentação legal, prever os usos e os limites judiciais da utilização desse tipo de instrumento. O Policial Militar 7 chega a comparar a ideia do uso das ferramentas tecnológicas com um carro descendo uma rua sem freios, para justamente ressaltar a necessidade do controle.

No mesmo sentido, o interlocutor do Ministério Público Federal diz que:

> Em primeiro lugar, eu gosto de começar esse assunto dando um passo atrás. A tecnologia, ela está na nossa vida. Os celulares na mesa não me deixam mentir. Em todos aspectos da nossa vida, na verdade, hoje em dia a gente é muito tecnológico dependente. *A investigação, ela não poderia ser diferente, são ferramentas que a gente utiliza e a gente vem tentando incorporar, não sem um atraso em relação a tudo que acontece no poder público, na burocracia, ela leva um pouquinho mais de tempo*. Então, assim, a gente tem um certo atraso em relação a isso, *mas a gente tem tentado incorporar essas tecnologias nas investigações, por duas notas. A primeira nota é que em qualquer corporação ela sempre tem que ter, ser feita a partir do marco das garantias do processo, das garantias constitucionais, essa é a primeira nota. Então, assim, a gente tem que ter uma questão assim de, vamos dizer assim cadeia de custódia, de grau de escrutínio*. No processo penal a gente tem uma situação que é a seguinte: toda prova produzida pode não estar sendo escrutinada na hora, porque, enfim, em uma interceptação telefônica — para falar de um recurso um pouquinho mais antigo ou alguma coisa assim —, mas ela será escrutinada e elas são escrutinadas, **então, essa é um marco que têm que guiar a incorporação de uma tecnologia nova** (Procurador da República, grifo nosso).

Nota-se, portanto, novamente, aqui em outra instituição, a mesma preocupação com princípios democráticos constitucionais. É preciso ressaltar, no entanto, que não fizemos observações empíricas, apenas entrevistas, então o que destacamos aqui é apenas o que nos foi dito. Se o que foi dito corresponde, na prática, a ações orientadas por essa lógica, não poderemos afirmar neste relatório. Tal preocupação pode ser, inclusive, objeto de investigações futuras.

Nas entrevistas realizadas, os interlocutores destacaram diversos usos das ferramentas tecnológicas no fazer da segurança pública. Assim, com frequência,

foi citado o uso da tecnologia para tornar mais efetiva a persecução criminal, com exemplificação de diversas tecnologias, como o GPS, o videomonitoramento e a quebra do sigilo telemático com o acesso aos dados do celular dos investigados. Também foram citados os usos da tecnologia que impactam diretamente a forma como o trabalho é feito e organizado no interior da instituição, desde ferramentas simples, como o uso do WhatsApp para as comunicações internas, principalmente da polícia militar. Um terceiro uso descrito também em grande parte das entrevistas foi a utilização de tecnologias para ações preditivas a partir de recursos de inteligência, que aparece também atrelado ao primeiro ponto da investigação criminal.

Por ser categoria nativa, transcrevemos aqui a fala do Policial Militar 7 sobre o que é a inteligência e como ela se relaciona com o tema da tecnologia:

> A atividade de inteligência, ela tem a função de assessorar. É muito comum a senhora ver na imprensa: "faltou inteligência". Todo mundo, né? Sem inteligência não se decide nada. A inteligência é uma forma de estruturar dados para processo decisório. Você vai decidir com mais qualidade. Por isso que é importante. O que é inteligência? É você conciliar memória com raciocínio. Banco de dados, historicamente dos acontecimentos. Como é que aquela organização criminosa atua naquela área? Historicamente você tem o processo algoritmo daquela organização… funciona assim: braço operacional, braço político, lavagem de dinheiro, daí você tem aquela situação já montada. E aquilo ali, ao longo do tempo vai mudando. Modus operandi… e aí quando você tem aquele quadro já montado no banco de dados, você faz o raciocínio. Você tendo conhecimento, como é que ela atua? Ah, ela atua aqui, então você já pode alocar o policiamento. Olha, essa facção ela é ligada a outra favela, então quando eles roubam carro, ou alguma coisa, o trajeto é esse aqui. Começou a roubar muito carro num tal lugar, opa! Isso aqui é o *modus operandi* da facção. Bota o policiamento nesse local que eles escoam pra cá. Então é muito dinâmico, e aí é que tá. Eu sou do tempo em que a gente era da máquina de escrever. Você dependia muito do elemento humano. Eu digo do elemento humano porque você depende da memória dos agentes, então quando você já tem aqueles agentes antigões, aí eles: "Ah, eu já sei". Aí dependia muito dessa parte, hoje em dia e ao longo do tempo, esses agentes continuam sendo muito importantes, só que eles aumentam a capacidade de raciocínio deles — porque eles têm a ferramenta, já não

> depende muito da memória, ele tem tudo ali — e ele vai tudo eletronicamente. Com planilhas, com tudo. Então, é tipo assim, pra quem gosta de uma atividade intelectual, é como se fosse uma cachaça. Principalmente quando você pega um caso pra tentar identificar, é gostoso trabalhar (Policial Militar 7).

Vimos, em conclusão, os conceitos e preocupações mobilizadas pelos próprios interlocutores quando questionados de forma geral sobre a temática da tecnologia na segurança pública.

Empecilhos à implementação das tecnologias

Neste momento gostaríamos de explorar aquilo que nossos interlocutores apresentaram como problemas ou desafios à incorporação de tecnologias no campo da segurança pública. São entraves de diferentes categorias, que apareceram em diversas entrevistas em certo momento do diálogo, o que nos fez perceber como as diferentes instituições lidam com questões muitas vezes semelhantes e como esse processo de inclusão tecnológica das atividades de segurança não é linear. Nesse sentido, notamos que muitas ferramentas são testadas, mas nem todas se encontram aptas para serem utilizadas na prática.

Assim, temos desde problemas que poderíamos chamar aqui de "operacionais" na implementação das ferramentas tecnológicas, que os entrevistados listam como custo financeiro ou força de trabalho sem treinamento específico para lidar com a área de tecnologia, a questionamentos políticos e morais do uso da tecnologia para controle e segurança. Nos tópicos a seguir, separamos essas questões para organizarmos a análise.

"Não espere que eu vou chegar aqui com uma Ferrari pra você, se você não sabe dirigir um fusca"

Os entrevistados citaram como um desafio em comum às diversas instituições, como o Ministério Público Estadual, Federal e, principalmente, as polícias militar e civil, o despreparo da força de trabalho atual para lidar com a tecnologia. Um dos entrevistados, Procurador Federal, assim colocou o problema: "Existe a questão da inclusão digital. E isso eu falo até dos colegas mesmo. São ferramentas que nem sempre são tão intuitivas assim de você utilizar. Então assim: você tem que ter alguma proficiência." (MPF1)

Um dos policiais militares entrevistados, por ter ocupado durante muitos anos cargos de gestão dentro da polícia, citou por diversas vezes na entrevista o problema de não possuir uma força de trabalho qualificada para desenvolver e operacionalizar sistemas tecnológicos com proficiência. Inclusive, a frase que dá título ao tópico pertence a esse interlocutor, ao responder que o maior problema que ele percebe na polícia militar, mais do que a falta de tecnologia, seria a "falta de gente capacitada" (Policial Militar 1).

Essa falta de pessoal capacitado seria, conforme delegado da polícia civil entrevistado, estrutural: "A gente não tem a cultura, e não é culpa individual de nenhum gestor, não. É que nós não temos tempo de parar em nos capacitar, porque a falta de estrutura, existe uma falta de estrutura, uma carência muito grande" (Delegado Civil 1).

É importante ressaltar novamente que a maioria de nossas entrevistas nas polícias militar e civil foram realizadas com oficiais do alto escalão da polícia, com seus gestores, e não com agentes de segurança pública que estão na linha de frente da atividade policial. Assim, essa problemática da capacitação do pessoal surgiu em diversos discursos, motivadas por explicações de duas naturezas: uma mais generalista, e que em nossa análise desdobramos para a questão da desconfiança depositada no trabalho policial, e a outra relativa à formação dos quadros da polícia com a exigência de formação em direito.

A primeira delas centrava-se numa justificativa pautada num comportamento tido pelos interlocutores como bastante comum às pessoas, que se relaciona com uma tendência a resistir a qualquer mudança. Veja a fala do Policial Militar 2:

> Porque é do ser humano, todo mundo é resistente a mudanças. Então, um exemplo bem bobo, o policial achava que o melhor carro era o carro com câmbio manual. Até que chegou o primeiro carro automático, o policial não gostava, porque achava que o carro não andava etc. Qual a solução para isso? Mudar conceitos, realizar treinamentos… eu fui responsável por isso no MJ: capacitar o militar a receber essas novas tecnologias (Policial Militar 2).

Nesse trecho, a explicação do entrevistado é que o comportamento de resistir ao novo seria natural ao ser humano e que, então, a própria instituição seria responsável por treinar e demonstrar aos policiais as funcionalidades e melhorias que seriam proporcionadas com o uso das novas ferramentas tecnológicas. Essa fala é interessante, pois por meio dela podemos perceber que a incorporação de uma ferramenta tecnológica não é apenas um problema técnico, no

sentido de ter um pessoal formado para utilizar e operar a tecnologia, mas que a própria inclusão da ferramenta altera as rotinas de trabalho, ou seja, reorganiza a forma como o trabalho cotidiano é realizado. No próximo trecho isso é explicitamente dito pelo policial entrevistado; vide a seguir os grifos que fizemos:

> Outro exemplo, esquadrão antibombas de PE. A gente tem uma PM com esquadrão antibombas — aqui é a PC. Só que antes o policial ia na braveza desativar a bomba. Agora chegou o robô… treinamento, treinamento… *Mas não é só treinar o robô, tem que mudar a concepção, as rotinas… Qualquer aparato tecnológico tem que mudar a rotina* (Policial Militar 2, grifo nosso).

Em entrevista com o Delegado Federal 1, ele fala de sua experiência com as polícias estaduais e reforça o argumento da resistência ao novo, chamando atenção para o componente do comodismo do policial em ser servidor público. Destacamos que essas opiniões são aqui apresentadas não no sentido de validar esses argumentos, mas numa análise compreensiva de como operam as representações sobre os atores e as diferentes instituições que se relacionam na produção da segurança pública e da justiça criminal. Nesse contexto, o Delegado Federal 1 declara:

> Existe também uma resistência dos policiais às novas tecnologias, porque tem que sair da zona do conforto, né. Aí a gente tem que pensar naquela questão do serviço público barra serviço privado. A realidade é que no serviço público se o cara não fala um português claro, não fizer nenhuma merda, ele não vai pra rua e vai ter o mesmo salário dele no final do mês. Então às vezes pro cara é mais fácil ele não queimar neurônio, não aprender a operar uma nova tecnologia, é mais sempre "o meu jeito é o melhor", é, a velha guarda, do que se modernizar e tudo mais, e sem dúvida há uma resistência. E o que acontece também, é que assim, como o número, em todas as… em todas as forças de segurança, se não em todas, na maioria, se entende que o número de policiais é menor que o necessário né. Então o… há muita, há muita circulação das pessoas pelas áreas né, dificilmente você consegue fixar pessoas ali na área de utilização das ferramentas tecnológicas mais modernas. Até porque, é isso… ah quem é assim… tem os polícia né… "polícia, meu, polícia, vamo pra rua, vou prender todo mundo", assentar a bunda na cadeira pra entender e pra mexer naquelas coisas nem todo mundo quer e tem muita movimentação (Delegado Federal 1).

Como pode ser percebido, ele categoriza também uma imagem de um tipo de policial que seria resistente à adoção das ferramentas tecnológicas e ao trabalho de inteligência e investigação, ligando esse perfil à atividade de operações nas ruas. Mais do que um tipo específico de policial, essa fala descortina uma perspectiva de imagem de como o policial é visto.

Essa questão ganha outra camada com a fala do Policial Militar 2, que segue explicando as "resistências à tecnologia". Ele continua sua análise tocando em um segundo ponto muito importante: como ele entende a resistência do policial militar das patentes mais baixas em aderir ao discurso tecnológico. Observe que, nesse momento, a explicação naturalizada de que "pessoas não gostam de mudanças" é recheada por uma outra explicação derivada do contexto socioinstitucional da polícia:

> A primeira coisa que você ouve o policial na ponta da lança falar é "olha, estou com essa câmera, mas vou quebrar a câmera porque vou levar tiro, vou pular muro, vou entrar na água, *aí vou responder ao IPM*…"…. Aí onde que contribuiu isso**?** *O policial vai ter a mesma segurança para atuar com o peito liso, ou com um equipamento que ele acha que custa milhões ou alguma coisa desse tipo?* Então isso aí vai interferir no psicológico e na ação do policial, então tudo isso aí tem que ser visto. E a gente só vai ver com treinamento. Chegou material, a primeira coisa a fazer é colocar o policial em sala de aula e explicar a importância daquilo. Depois, operar aquilo, treinar, exaustivamente, até ele sentir confiança com o equipamento. […] (Policial Militar 2, grifo nosso).

Assim, o medo do policial em ter seu trabalho fiscalizado ou de danificar o equipamento e ser responsabilizado por isso aparecem como explicações menos generalistas da resistência à utilização das inovações tecnológicas. Nesta mesma entrevista, um outro interlocutor assim explica:

> Eu tenho uma teoria, baseada no meu entendimento. O Policial Militar associa a nova tecnologia à ponta, à fiscalização, então em um primeiro momento ele resiste. *Ele acha que aquilo é para fiscalizar*, como a bodycam e o GPS. Em um primeiro momento, parece ser só fiscalização, até que comece a entender a finalidade. É uma barreira que precisa ser quebrada (Policial Militar 5, grifo nosso).

Dessa forma, a dificuldade inicial não estaria ligada somente a uma resistência humana ao que é novo, mas, na perspectiva dos policiais entrevistados, se

relacionaria ao medo do policial diante de uma desconfiança social, mas também, institucional a respeito de seu trabalho. Inclusive, a desconfiança da população em relação à polícia é tema sociológico que vêm sendo pesquisado no exterior e no Brasil (Oliveira Junior, 2011; Tyler, 2004), com pesquisas que investigam as interações entre percepções difusas e específicas sobre violência policial, abordagem e eficiência na construção da imagem construída sobre a polícia.

Neste ponto, segundo fala de representante da polícia civil, seria preciso questionar se a própria sociedade está apta a lidar com a transformação digital da segurança pública: "E aqui no Rio de Janeiro, então? Será que a sociedade está preparada para ter uma polícia que busque a justiça, que seja independente, que faça a coisa acontecer?" (Delegado Civil 1). Isso porque, segundo esse mesmo delegado: "A polícia é para proteger o sistema. Se você quer contestar o sistema, e o sistema... Se você evoluir muito a polícia, você quebra o sistema. E quem controla, quem é o detentor do poder, não quer que quebre o sistema" (Delegado Civil 1). Há, portanto, uma forte preocupação por parte do agente de segurança pública com os entraves à ação policial decorrentes de uma tentativa de manutenção do *status quo* por parte de determinados membros da sociedade.

Por outro lado, Kant de Lima (2010) destaca o caráter hierarquizado do sistema judicial criminal no Brasil, que combina uma série de princípios distintos na produção da verdade jurídica. Esses paradoxos funcionam como empecilhos para a compreensão totalizada do sistema, o que resulta em sua fragmentação institucional e na segmentação hierárquica de atores e instituições que o compõem. Ao invés de questionar a lógica paradoxal, os atores institucionais acusam-se mutuamente, delegando às outras partes a responsabilidade ou culpa pelo mau funcionamento do sistema (a lógica da culpa e do castigo em vez da *accountability*). Conforme Kant de Lima (2010, p. 16): "Esses ruídos, produzidos entre as diferentes partes do sistema, que agem de acordo com lógicas distintas, afetam profundamente sua credibilidade e, portanto, sua eficácia institucional, criando um clima de desconfiança na sociedade como um todo". Isso é notado por um dos delegados da polícia civil entrevistados, para quem há um perceptível conflito entre os três poderes:

> Então, tem essa perspectiva dos três poderes que estão em conflito atualmente. Não é segredo para ninguém. Isso atrapalha também, que a falta de harmonia entre os poderes, acho que é o pior dos fatores para a segurança pública, porque a gente acaba não conseguindo aplicar nenhum

> daqueles condões da pena, por exemplo, da ressocialização, da prevenção, da desestimulação. Nada disso funciona, porque os poderes estão brigando (Delegado Civil 2).

Ainda sobre a questão da desconfiança depositada no trabalho da polícia, um dos nossos entrevistados, identificado aqui como "ordem pública", pois trabalha na Secretaria de Ordem Pública do Rio de Janeiro, diz que:

> […] mas esse é um desafio que é necessário; na minha opinião já é urgente, né? Acho que você resgata muito da legitimidade da polícia com esses movimentos, porque hoje a polícia ou agente de fiscalização, a guarda né? Podendo colocar como um, no mesmo guarda-chuva, hoje você tem uma crise de legitimidade, né? As pessoas não se sentem protegidas por esses atores, as pessoas se sentem aviltadas por esses atores na maioria das vezes, né? Claro que tem de tudo, mas é… eu me vi eu… como gostei… gostava muito de trabalhar na rua né? Investigando, fazendo, indo cumprir mandado de prisão, buscar apreensão das investigações… é muito sintomático isso. As pessoas, elas desconfiam muito, né? Tem pesquisas inclusive que denotam esse tipo de desconfiança (Ordem Pública).

Outro ponto citado em nossas entrevistas foi a questão da carreira dentro da instituição e da reserva do campo aos profissionais da área do direito, atores que em sua formação universitária não possuem treinamento para lidar com gestão de dados ou tecnologias. Em relação à polícia militar, essa crítica foi realizada por um interlocutor interno.

O Policial Militar 1 nos relatou como um problema que a formação em direito seja exigida como requisito para ingresso na instituição. De acordo com sua explicação, a PM do Rio de Janeiro é uma instituição grande que abrange uma série de atividades para além de sua atividade-fim, que seria o policiamento ostensivo, como a própria atividade de administração dos recursos e pessoal da corporação.

Assim, a carreira ser exclusiva de profissionais com formação em direito não atenderia às necessidades práticas do dia a dia. A seguir, sua análise:

> […] eu não tô olhando só a minha atividade-fim, eu tenho toda uma estrutura por trás desses caras que tão na rua que dá um suporte pra que aquele serviço aconteça. E é justamente uma estrutura baseada em quê? *Em gestão, em formação, uma gama de conhecimentos que nós temos aqui que nós temos que selecionar pessoas que entendam ou que*

> *gostem, ou que se interessaram por aquilo e o cara tá fazendo*. Eu fui um exemplo disso mesmo. *Na minha academia não fiz Direito, eu fui fazer Administração e segui minha carreira toda nessa área nas pós, mestrado, doutorado eu fiz na parte de pesquisa operacional*. Então assim: me deu uma visão excelente da Instituição, tá? *Ao contrário dos meus colegas todos que fizeram Direito, e o cara só pensa em processos. A cabeça do cara é processo, é prender, é corregedoria*. Falei, cara isso aqui é legal, *mas eu não preciso ter todo mundo pensando dessa forma*. Não dá pra ter todo mundo pensando dessa forma. Quem é que vai fazer a parte que eu tenho que fazer pra tocar a Instituição, né? Então eu tenho essas… essa dificuldade. […] Porque já é da natureza deles, um cara que fez engenharia, um cara que fez uma outra, cara, e tentar se enquadrar na Instituição naquilo que ele faz e vai nos ajudar bastante. Como Instituição, vai nos ajudar muito. *Mas aí no meio do caminho houve ali um golpe de Estado e os caras disseram "nananão, libero somente bacharel de Direito", mudaram lei, fizeram um negócio bem fechadinho, que hoje pra eu mudar politicamente não tô conseguindo*. Dei essa ideia de mudar, de abrir. Aí o secretário tentou, aí eu falei poxa, a coisa tá tão complicada pra gente, eles amarraram tanto que eu não consigo mudar. (Policial Militar 1, grifo nosso).

Portanto, de acordo com esse interlocutor, os quadros da instituição necessitam de profissionais com formação variada, como engenheiros, administradores, profissionais com formação em tecnologia da informação, entre outras especializações necessárias na organização do trabalho. A mesma percepção é manifestada pela polícia civil, que aponta que os concursos para a instituição focam em matérias de direito (penal, constitucional, entre outras), em detrimento de conteúdos relacionados à tecnologia. Assim, um dos delegados entrevistados afirma:

> Então você não tem, por exemplo, na prova, exigência de nada em termos de lógica de programação, de nada em termos de análise de vínculos, de nada em termos de banco de dados […] Então eu acho que teria que haver um redesenho nessa matriz, para a gente recrutar pessoas com essas competências que a gente julga hoje importantes (Delegado Civil 2).

Um dos interlocutores da polícia militar ainda ressalta o problema em fixar em cargos os policiais que vêm com formação em direito, tanto pela característica de um perfil de "concurseiro" e de ter um horizonte de possibilidades de carreiras

em outros cargos públicos com melhores remunerações quanto pelo trabalho que não tem relação exclusiva com a assessoria jurídica da polícia. Vejamos:

> Desse quadro eu tenho duas questões: beleza, você não vai fixar gente aqui dentro, que a maioria do pessoal que entra por concurso aqui, *eu acho que na primeira turma metade foi embora no curso, porque já tinham passado pra outros concursos, foram chamados, metade foi embora*. Da outra metade, eles acharam que ia ser assessoria jurídica. Quando eles descobriram que eles não iam pra assessoria jurídica, aí você tem uma crise com os garotos, você vai por idade, você vai fazer a mesma coisa que aquele garoto de nível médio que se formou faz, que o tenente faz. O que é que um tenente faz, o que é que um capitão faz? Então você não vai passar perto da assessoria jurídica, ah mas nem sonhando. O máximo perto que você vai chegar é na seção de justiça e disciplina [...] mas se você tiver tantos formados, só vai ter vaga pra 1. E uma vaga por unidade, quando eu tenho uma turma grande, eu não tenho vaga pra todo mundo pra isso, eu tenho meia dúzia de caras na assessoria, aí todo mundo aqui criou, começou a criar, "ah eu quero um garoto desse, formado em Direito, pra resolver um problema que já existia". Eu falei assim: "Pô cara, se você tirar o garoto formado agora e botar aqui, eu não tenho tenente na rua. *Eu tenho outro problema institucional, eu não tenho duzentos caras, pra você tirar dez caras e botar aqui dentro, eu tenho trinta, com a necessidade de cem, né? Então criou essa dificuldade. As outras turmas seguiram, nós estamos na segunda, terceira turma, segue o mesmo padrão"*. Entra um quantitativo, os caras olham, passam num concurso, saem e sem contar que vão estar aqui dentro, né. O nível de salário de um cara formado em direito, pro cara que tá sem emprego, tá ótimo. Mas quando a gente chega aqui, consegue um salário, consegue um emprego e começa a estudar paras as coisas que ele gostaria de fazer, as oportunidades de salários são muito infinitamente maiores, para aquela, ele vai ganhar de inicial, às vezes em algumas áreas, o que eu ganho em final de carreira aqui. Ele passa pra promotor de justiça e vai ganhar de inicial o que eu ganho no final. É que vai embora, *você não vai fixar esse cara aqui. Mas nem sonhando você fixa esse cara aqui; pra mim é um cara temporário. Ao longo de trinta anos, não vai, a maioria, é que eu não vou estar aqui pra ver, espero estar vivo pra ver, fazer essa conta, de quem entrou há vinte anos quantos eu ainda tenho aqui dentro?* (Policial Militar 1, grifo nosso).

Essas falas refletem sobre problemas institucionais internos na formação dos quadros de carreira das polícias militar e civil, que se entrelaçam com a temática da utilização ou não de ferramentas tecnológicas, uma vez que dizem respeito à formação da carreira policial, temas também destacados pelo Delegado Federal 1:

> Assim, havia o treinamento, e nem sempre a pessoa que estava sendo treinada era a pessoa que estava à frente do projeto depois. E depois, quando estava no projeto, ficava um, dois, três meses e saía. *É uma rotatividade muito grande e uma falta de treinamento*. Porque as pessoas que entravam depois… porque por exemplo, né, aí falando como funcionava, porque deve ser uma coisa muito similar agora. Porque quando a gente compra o software, junto com o software vem um número X de treinamentos. Então, a partir, sei lá, vêm cem vagas de treinamento. Então você treina cem pessoas, a pessoa cento e um, tem que ser feito o pagamento desse treinamento. E na maioria das vezes não há o investimento por parte aí do Estado nesse treinamento adicional. É…, então é isso, o que a gente via muito era isso, *é que tinha muita rotatividade e depois, as pessoas novas que chegavam não eram treinadas, porque as vagas já tinham acabado e não tinha investimento do Estado*. Então ficava muito no "querido amigo explicar como é que era" e aquele negócio é difícil, é chato e aí vai ficando (Delegado Federal 1, grifo nosso).

É interessante notar, assim, a proposição feita pelo interlocutor da polícia civil, que afirma que: "[…] a forma para resolver isso, não sei se seria aplicar isso genericamente ou ter concursos para policiais com uma formação específica na área de tecnologia. Eu não sei, não me lembro ainda sobre o assunto. Mas seria bom…" (Delegado Civil 2).

De acordo com a fala do Promotor de Justiça 2, no Ministério Público do Rio de Janeiro não haveria uma capacitação que nivelasse os profissionais a trabalharem com a tecnologia. Assim, os manejos e conhecimentos sobre as ferramentas tecnológicas partiriam das aptidões e interesses pessoais de cada promotor de justiça, como observa-se no seguinte trecho:

> E aí isso, *não existe eu acho um nivelamento institucional, em nenhuma esfera*. É… no (...), por exemplo, a gente tem primado pela capacitação dos colegas. Nós somos poucos dentro do (...), mais ou menos em torno de 28 colegas e aí…usualmente, a gente tenta trazer capacitação para todos eles com as novas ferramentas, e assim a gente trabalha. *Mas ainda*

> *assim, o nivelamento, ele não existe. Isso depende; cada colega tem um grau de aprofundamento na matéria diferente do outro*. (Promotor de Justiça 2, grifo nosso).

Da mesma forma, o Policial Militar 6 explica que, conforme seu ponto de vista:

> Uma nova tecnologia muda tudo, e não só aqui na polícia militar, no serviço público em geral, o servidor público tem que se adaptar. Tem que conhecer, tem que fazer curso. Pra você ter uma ideia, eu sou da época em que não existia celular. O batalhão tinha três telefones. Era o 23 ali no Leblon que eu trabalhava, né. Tinha três telefones no batalhão. Eu saía de casa, tipo assim, mil pessoas com três telefones: que um era da sala de operações, outro era da manutenção e outro era do comandante. Pra comunicação externa. Então o primeiro celular que eu tive foi em 98/99. Então eu ia para faculdade, biblioteca né. Quando começou essa enxurrada tecnológica, aí eu fui a reboque. Tive que fazer curso de Word, Windows, pra aprender a mexer com, né? Só que no mundo moderno a velocidade é imensa. Aí infelizmente a gente fica pra trás, né? A nova geração de oficiais que vêm chegando elas tão chegando conectadas, né? Mas os servidores que estão aqui eles precisam da atualização profissional. Porque a gente não entende (Policial Militar 6).

Ao mesmo tempo, é interessante notar que, apesar da ausência de treinamento institucional, o Promotor de Justiça 3 afirma que:

> Tecnologia mudou totalmente o nosso trabalho. No passado, utilizávamos quase nada de tecnologia, porque nós tínhamos em regra, a folha penal do indivíduo, que era feita manualmente, nós tínhamos as perícias que eram, também, praticamente, todas manuais (Promotor de Justiça 3).

Em um longo relato, o mesmo interlocutor segue descrevendo diversos recursos que foram incorporados à investigação criminal, como o DNA, a triangulação pelos aparelhos celulares, o GPS, o Luminol, entre muitas outras ferramentas incorporadas à atividade de investigação. Ele descreve também impactos menos aparentes da tecnologia a um observador desatento, como a possibilidade do trabalho *home office,* que agora permitiria que o promotor se ausente da comarca em que está lotado. Nesse relato, percebemos que essa dimensão de constante transferência de um local para outro, muitas vezes em comarcas pequenas e do interior, em se tratando de promotores recém-concursados, aparece como um desafio do trabalho. Ele diz:

> Eu acho que vai voltar, porque a gente precisa voltar, mas vai ser mais ou menos híbrido. Você vai lá duas vezes por semana, vai ser uma acho eu, né? Acho eu. O corregedor nacional do Ministério Público quer que todos voltem. Mas por exemplo, Minas Gerais, está acontecendo uma coisa interessantíssima, como é um estado muito grande, as pessoas, os promotores eram obrigados a morar na comarca. Com a pandemia, eles estão morando nos centros regionais e a produtividade aumentou. Então você vai mandar o cara de novo para o interior de Deus me livre? Eu fui promotor em Minas. Eu chegava em São João Del-Rei, pegava um ônibus até perto de Tiradentes para ir a Prados, numa estrada de terra. Prados é onde você já deve ter ido. Bichinho. Todo mundo já foi a Bichinho. Bichinho era minha Prados. Porra, no meio do nada. Eu ia enlouquecer se eu ficasse lá. (Promotor de Justiça 3)

Percebemos, então, pela fala dos interlocutores que a questão da implantação das ferramentas tecnológicas caminha em conjunto com preocupações sobre a organização das instituições e das rotinas de trabalho dos atores. Questões relativas à confiança do trabalho policial, portanto, ao controle do trabalho, como também aos treinamentos específicos para lidar com cada uma dessas ferramentas são tópicos abordados pelos nossos interlocutores como desafios da implementação das tecnologias na área da segurança pública.

Gostaríamos de ressaltar também que a frase que dá título a este tópico, "Não espere que eu vou chegar aqui com uma Ferrari pra você, se você não sabe dirigir um fusca", expõe ainda uma visão de que o aparato tecnológico, aqui chamado comparativamente de "Ferrari" para ressaltar sua boa qualidade, é tido como um produto concluído, como o resultado de um projeto de desenvolvimento que entregou, por fim, uma mercadoria em pleno funcionamento. Ela esconde, por exemplo, que o desenvolvimento de sistemas e ferramentas na área de tecnologia da informação é um processo contínuo de avanços, retrocessos e de escolhas que em muitos aspectos produzem efeitos políticos e práticos na realidade.

Os sistemas são constantemente transformados pelos usuários, numa criação muito mais colaborativa do que a frase permite imaginar. Esse ponto não passou despercebido por todos os nossos interlocutores, como ocorre na fala do Promotor de Justiça 1, que destaca:

> Eu vi isso acontecer várias vezes, eu estive na tecnologia mais de uma vez nos últimos oito anos. Em todas as vezes, novas soluções enfrentavam o mesmo problema. As pessoas acham que estão comprando carro na concessionária, você compra um carro, chega, você liga e ele funciona. Não dá problema, é muito raro. *Quando você compra uma ferramenta dessas, é que nem encaixar um círculo num quadrado. Tem muita coisa para ser feita de modo artesanal. As pessoas não entendem que a tecnologia é artesanal*, em muitos aspectos. Os códigos não se encontram como num quebra-cabeça, eles têm que ser lapidados, encontrados. *E você acaba implementando, num processo de tentativa e erro*. Isso é inevitável. (Promotor de Justiça 1, grifo nosso).

No próximo tópico, abordaremos outra dificuldade também citada por interlocutores de diferentes instituições, o que nos possibilita dizer que é um problema compartilhado pelo sistema de justiça criminal. Problema esse que, inclusive, tem relação com a própria nomenclatura aqui utilizada — "sistema" —, pois refere-se ao compartilhamento e integração de bases de dados.

"Ilhas de dados": a questão da integração

> "A grande verdade é que tem sim, ilhas de dados. Cada corporação entende que aquilo ali é sua fortaleza, e assim não quer compartilhar" (Policial Militar 4).

> "Todas as vezes que eu realmente tive problema em obter base de dados, foi quando as bases eram públicas. Requisições de dados privados eram mais fáceis de serem obtidas do que bases que tinham uma certa distribuição de feudos" (Promotor de Justiça 1).

Utilizamos essas frases para abrir a discussão em relação ao problema da integração como questão citada amplamente nas entrevistas. Observemos a escolha das palavras "ilha", "feudos" e "fortaleza", pois elas não se deram ao acaso. Todas elas remetem à imagem de áreas delimitadas por fronteiras rígidas.

A integração da forma como apareceu no relato dos nossos interlocutores diz respeito basicamente à interlocução de bases de dados. Mais do que somente o acesso e o compartilhamento dessas bases entre diferentes instituições, os entrevistados ressaltaram a importância e a necessidade

de que, em termos tecnológicos, essas bases falem a mesma linguagem: a "interoperabilidade".

O Policial Militar 3 assim conceituou a integração, diferenciando-a da interoperabilidade: "É, interoperabilidade seria mais se tivesse sistemas diferentes que você precisa adaptar para que eles operem juntos né?" A interoperabilidade seria a preocupação de que sistemas diferentes se comuniquem a partir de uma linguagem em comum. Por sua vez, de acordo com o Policial Militar 3: "A integração, na verdade, é uma troca de informação, né?" (Policial Militar 3).

Nesse contexto, então, aparecem duas categorias de problemas: a base de dados existindo, há a necessidade de que ela seja compartilhada entre as instituições para que o trabalho seja mais eficiente, no sentido de poupar o tempo de trabalho de reunir a informação. Então, na visão de vários de nossos entrevistados, é preciso, em um primeiro momento, que as instituições compartilhem os dados. Numa segunda categoria, temos o problema da linguagem tecnológica e dos softwares, pois é preciso que as bases de dados estejam produzidas em sistemas que sejam operáveis em conjunto, para que os dados migrados possam ser lidos e utilizados em diferentes instituições. Essa ideia é manifestada expressamente por um dos interlocutores da polícia civil, que afirma: "O que eu sinto falta, e isso para mim é um grande problema, é falta de uma uniformização nacional de dados" (Delegada Civil 3). Embora se reconheça uma tentativa de maior integração entre as bases de dados dos diferentes órgãos da segurança pública, isso ainda não seria, na visão de nossos interlocutores, suficiente:

> Hoje em dia, até o sistema está migrando para uma integração melhor entre o Judiciário, MP, a polícia, ainda não é boa, né? E essa questão nacional a gente sente muita falta, em termos de ter acesso ao histórico criminal daquela pessoa, um banco de dados com fotografia, a gente tem até o InfoSeg, que é um banco de dados nacional, mas, assim, CPF, não tem foto, só dá para ver pelo CPF, base no arquivo de endereço, não é tão bom assim (Delegada Civil 3).

O Promotor de Justiça 1, por exemplo, relatou que tem dificuldade em ter acesso às bases de dados de instituições públicas, pois, para ele, haveria uma "distribuição de feudos" entre os órgãos que produzem e armazenam os dados. Alertou que, muitas vezes, cada órgão constrói a sua base de dados e não a compartilha.

Ainda que haja algum tipo de compartilhamento, os dados são estruturados de maneiras diferentes, o que faz com que este interlocutor veja, portanto, carência nesse ponto, e a necessidade de "desdepartamentalizar" a tecnologia dentro das estruturas ministeriais, falando especificamente do caso do Ministério Público. Por fim, ele destaca que as bases que são consumidas, ou que teoricamente deveriam subsidiar essas ações, precisam estar interoperadas.

Uma delegada da polícia civil entrevistada destaca que há dificuldades de integração dentro do âmbito da própria instituição, quando se considera a necessidade de a PC de determinado estado da federação obter acesso a dados e informações de outros estados. Para a entrevistada, seria necessária uma uniformização a nível federal das bases de dados estaduais:

> Eu acho que deveria ser uma coisa de âmbito federal, porque há uma disparidade muito grande entre as delegacias, as polícias civis, ao longo do Brasil inteiro, então, algumas elas gozaram de um processo de desenvolvimento tecnológico mais precoce e outras mais tardias. Então, quando eu penso em uma integração dos bancos de dados, eu preciso que haja, primeiro, uma correspondência tecnológica e uma comunicabilidade entre os próprios sistemas. Então, eu não consigo vislumbrar isso seja realizado por força exclusivamente dos estados. Eu acho que teria que ser uma iniciativa nacional, tal como a criação do banco de mandados, o BNP, hoje em dia também tem o Banco Nacional de Medidas Positivas de Urgência contra Mulher, então, eu acho que teria que ser mais ou menos por aí, a criação de um grande banco de dados de âmbito nacional mesmo (Delegada Civil 3).

Da mesma forma, o problema da integração foi relatado pelos interlocutores da polícia militar, o que pode ser observado no diálogo a seguir, em que a pesquisadora enfatiza o tema pedindo confirmação da explicação:

> Policial militar 4: Via de regra, é complicada a integração.
> Pesquisadora: E não é necessariamente um problema de falta de tecnologia. É falta de integração.
> Policial militar 4 em conjunto com o Policial Militar 2: Isso, com certeza.
> Policial militar 4: Há muitas mudanças no estado, mudanças de cadeiras… aí tem que refazer as conexões. Por exemplo, se for na Prefeitura do Rio… eu brincava que sou PM; servi lá cinco anos, e voltei. Quando voltei, foi um choque. Um documento levava um mês para enviar um decreto

> da prefeitura para a PM, e isso porque era tudo eletrônico. Em geral, a integração é ruim (Policial Militar 4).

Em mais de uma entrevista, os atores afirmaram que a ausência de integração não é um problema de falta de tecnologia, mas sim um problema institucional, identificado por eles como disputas de poder sobre os dados e sobre as informações. Em pesquisa anterior, em que tratamos exatamente da questão da integração das instituições no sistema de justiça criminal no Rio de Janeiro (Bottino *et al*., 2020), observamos que os obstáculos para a integração se originam também da construção histórica de um distanciamento entre as forças policiais no estado do Rio de Janeiro, que resultou na criação de culturas institucionais próprias e de difícil interconexão.

Este fator resulta em práticas de integração escassas e baseadas na pessoalidade e confiança mútua entre atores específicos, que não se mantém caso essa sinergia entre os integrantes das forças policiais deixe de existir. Portanto, a pesquisa (Bottino *et al*., 2020) concluiu que, quando há integração, trata-se muito mais de um movimento de cunho pessoal do que institucional.

Indícios disso apareceram na entrevista com o Policial Militar 3, quando ele comenta sobre a integração entre a polícia militar e civil para uma operação teste da tecnologia de reconhecimento facial na cidade do Rio de Janeiro. Ele diz:

> A integração hoje, ela é mais física né? Aqui no Rio ela é física, por exemplo, quando a gente fez lá o teste de reconhecimento facial. [...]. E essa cooperação técnica continha tanto a polícia militar quanto a polícia civil. Naquele momento ali, a gente tava atuando integrado, mas mesmo essa integração, ela foi mais física do que integrada de fato. Por quê? A gente não detinha o banco de dados da polícia civil, esse banco de dados não era do, da ação conjunta. Era o banco de dados da polícia civil e o banco de dados da PM, e pronto. Entendeu? Quando precisava de alguma coisa, eu tinha que ir na polícia civil, "oh, surgiu um alerta aqui, confere?" (Policial Militar 3).

Esse interlocutor segue descrevendo como o problema da consulta ao banco de dados da polícia civil foi resolvido acrescentando-se um policial civil à operação, e não com o fornecimento do banco de dados. Ele continua explicando o que aconteceu:

> Aí a gente passou a tentar automatizar esse processo. Não é dando um jump da triagem do policial civil, mas a gente colocou um policial civil na linha de frente. A gente pegou, pô, pega alguém do DRC e bota aqui dentro aqui, na operação pra ele ficar olhando pra câmera, pra ele poder dizer, entendeu? Então assim, coloca um policial numa operação aqui e ajuda na triagem, né? Mas de qualquer forma, essa integração ela ocorreu mais fisicamente do que sistemicamente, entendeu? Fica melhor explicar assim. Entendeu? A nível de sistema ela praticamente não chegou a ser operacionalizada (Policial Militar 3).

Fica expresso que o problema da integração das bases de dados e do compartilhamento da informação foi driblado situacionalmente a partir das relações entre os atores. O ato de "chamar alguém", provavelmente alguém em quem se confiava, para participar em conjunto da operação da polícia militar. Essa é a "solução" apresentada por uma delegada da Polícia Civil entrevistada, que fala em "relações pessoais":

> O que eu vejo muitas vezes é a questão de relações pessoais mesmo, entende? Então, por exemplo, eu sempre tive um trabalho muito próximo com a polícia militar porque eu acho importante. Então, essa coisa de boca a boca, "ah, tô com esse problema aqui e tal", "vamos ajudar", a gente resolve (Delegada Civil 3).

Assim, o relatório produzido em 2020 observou também que as diferentes culturas institucionais e uma possível competição desencadeiam conflitos no que se refere às atribuições específicas de cada instituição no campo da segurança pública, dificultando, assim, a integração.

Nele, explicou-se que: "Eventuais disputas institucionais também podem ser entendidas como um dos fatores explicativos para a resistência das instituições em compartilhar informações, para com isso construir uma gestão integrada de dados." (Bottino *et al*., 2020, p. 142). Essa ideia da competição aparece aqui novamente nas falas dos entrevistados, ao relacionar as bases de dados com "fortalezas" e "feudos", territórios que devem ser protegidos do acesso de um possível inimigo. Veja a fala do Policial Militar 2, na qual fica expresso que o problema da integração tem mais relação com vínculos políticos e institucionais do que com um possível problema de falta de tecnologia:

> Como o Major [...] falou, existem muitas ilhas de dados, então esse é um ponto importante [...]: definir como compartilhar esses dados. Mas isso só

> vai ser definido quando as agências, as entidades sentarem juntas e discutirem isso. Aqui a gente faz isso, a gente aqui reúne defesa civil, bombeiros, agora o pessoal do metrô, outras secretarias além da secretaria de segurança pública. E a gente começa a discutir isso. Nossa secretaria começou a fazer isso, agora de forma oficial. E aí os problemas vão aparecendo, mas também as soluções (Policial Militar 2).

Como ponto de comparação por contraste, os interlocutores, principalmente os da polícia militar — mas também o agente da secretaria de ordem pública — citaram o modelo utilizado pelo Ceará como exemplo positivo de uma gestão integrada da segurança pública. Nesta fala do Policial Militar 3, é possível perceber que a principal dificuldade estaria na comunicação entre as instituições para o fornecimento do *webservice*[35]:

> E quando eu estava conversando com esse colega lá do Ceará, que ele falou sobre o nível de integração que eles estão. Eu perguntei a ele como eles fizeram isso, pra conseguir juntar todas, todos os, todas as bases de dados num *datahouse*. Primeira coisa é, todas essas bases precisam fornecer dados, então tem que levantar *web service* de todas elas. Agora a pré-disposição em fornecer *webservice* para que você dê os dados, é que é, acho, o grande entrave hoje, né. A gente no passado teve um projeto chamado ARGOS, isso lá em, nos idos de 2010 se eu não estou enganado. A ideia do ARGOS era exatamente fazer isso, integrar as bases de dados. Integrar as ocorrências da polícia civil com as ocorrências da PM, com os dados do Detran, basicamente, era isso. E aí faria uma troca de informações (...) (Policial Militar 3).

Portanto, apresentamos neste tópico a questão da integração a partir da perspectiva de nossos interlocutores durante as entrevistas, ou seja, como um problema que afeta diretamente o conceito de um sistema de justiça criminal. Percebemos também que ela ocupa um lugar central dentro do debate do uso de tecnologias baseadas em dados pelo Estado, remetendo, inclusive, ao próprio surgimento do direito à proteção de dados pessoais.

---

35 *Web service* é a ferramenta tecnológica que permite a integração de diferentes sistemas, viabilizando a comunicação entre aplicações diferentes. São funções de softwares que funcionam como uma espécie de tradutor entre diferentes linguagens de softwares, inclusive, remotamente. (WEB SERVICE. Disponível em: <https://gabrielpolo.medium.com/o-que-%C3%A9-um-webservice-c5104d847a85>. Acesso em 24 nov. 2022).

Isso porque, na paradigmática decisão do Tribunal Constitucional Alemão de 1983, sobre a chamada "Lei do Censo Alemã", considerou inconstitucional a lei de recenseamento que determinava a coleta compulsória de dados pessoais dos cidadãos, que seriam posteriormente analisados de maneira automatizada, bem como previa o compartilhamento desses dados entre os órgãos da Administração Pública.[36]

O Tribunal julgou que a coleta e o armazenamento ilimitado de dados pessoais da população, assim como seu compartilhamento indiscriminado entre os entes da administração pública, constituiria grave ameaça os direitos de personalidade das pessoas, reconhecendo, assim, que o direito fundamental ao livre desenvolvimento da personalidade envolve o direito do indivíduo de determinar o fluxo de suas informações na sociedade (Mendes, 2008).

É possível afirmar, assim, que a decisão do Tribunal Constitucional Alemão estabeleceu a necessidade de verdadeira "divisão informacional dos poderes", sendo fundamental a vinculação finalística dos dados (Wolter, 2018). Para Viana, Montenegro e Gleizer (2020):

> Alinhando ambas as considerações anteriores, a saber, de um lado, o necessário regramento das intervenções informacionais por área de atividade estatal e, de outro, a consequente vinculação às finalidades do levantamento, justifica-se a defesa da separação informacional de poderes. Isso significa que *é ilegítima uma base de dados comum a todos os órgãos estatais que armazene informações de inteligência e de segurança pública obtidas por autoridades dos mais diversos níveis*. (Viana, Montenegro e Gleizer. 2020, p. 37 grifo nosso).

Não deixa de chamar à atenção, portanto, o fato de haver, na prática policial, uma pretensão de compartilhamento de dados pessoais entre diferentes agentes e órgãos de segurança pública, o que iria de encontro à própria fundamentação do reconhecimento do direito à proteção de dados pessoais. O próprio Supremo Tribunal Federal tem decisões recentes nesse sentido, com destaque

---

36 Nas palavras de Menke (2019), "o ápice do reconhecimento da proteção de dados ocorreu com a decisão do Tribunal Constitucional Federal sobre a questão do censo demográfico que se realizava na Alemanha no ano de 1983 (Volkszählungsurteil). Esta decisão estabeleceu o direito fundamental à autodeterminação informativa (Grundrecht auf informationelle Selbstbestimmung)."

para o julgamento da Arguição de Descumprimento de Preceito Fundamental 722[37] e da Ação Direta de Inconstitucionalidade 6.529.[38]

"E aí a gente tem um problemaço": dados como ativos organizacionais

Uma menção recorrente nas entrevistas realizadas foi feita em relação à "falta de cultura de dados" dentro das organizações. Isso seria, nas palavras de interlocutor da polícia civil, o primeiro passo para a utilização efetiva de novas tecnologias da informação e comunicação pelas forças de segurança pública:

> Você tem que ter aqui, primeiro, uma mudança de cultura, uma transformação digital, para que você tenha o gestor voltado nas ações estratégicas dele, quando ele monta a estratégia da instituição, o dado tem que ser visto como um ativo institucional que vai gerar valor (Delegado Civil 1).

Reiteradamente, o delegado entrevistado se refere aos dados como um "ativo informacional", isto é, como um bem capaz de agregar valor à organização. Em suas palavras:

---

37 "Na ação, a Rede Sustentabilidade questionava investigação sigilosa que teria sido aberta contra um grupo de 579 servidores federais e estaduais de segurança e três professores universitários identificados como integrantes do 'movimento antifascismo'. A iniciativa do partido foi motivada por notícia de que a Secretaria de Operações Integradas (Seopi) do Ministério da Justiça teria produzido um dossiê com nomes e, em alguns casos, fotografias e endereços de redes sociais das pessoas monitoradas, todas críticas do atual governo, e distribuído um relatório às administrações públicas federal e estaduais." (STF. *STF julga inconstitucionais atos do Ministério da Justiça sobre dossiês contra antifascistas.* Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=487103&ori=1). Acesso em: 14 jun. 2023.

"O Tribunal, por maioria, julgou procedente o pedido formulado na arguição de descumprimento de preceito fundamental para, confirmando a medida cautelar deferida, declarar inconstitucionais atos do Ministério da Justiça e Segurança Pública de produção ou compartilhamento de informações sobre a vida pessoal, as escolhas pessoais e políticas, as práticas cívicas de cidadãos, servidores públicos federais, estaduais e municipais identificados como integrantes de movimento político antifascista, professores universitários e quaisquer outros que, atuando nos limites da legalidade, exerçam seus direitos de livremente expressar-se, reunir-se e associar-se, nos termos do voto da Relatora, vencido o Ministro Nunes Marques. Falou, pelo amicuscuriae Associação Direitos Humanos em Rede, o Dr. Gabriel de Carvalho Sampaio. Afirmou suspeição o Ministro André Mendonça. Plenário, Sessão Virtual de 6.5.2022 a 13.5.2022" (STF, ADPF 722).

38 "Por unanimidade, o Plenário do Supremo Tribunal Federal (STF) estabeleceu que os órgãos componentes do Sistema Brasileiro de Inteligência (Sisbin) somente podem fornecer dados e conhecimentos específicos à Agência Brasileira de Inteligência (Abin) quando comprovado o interesse público da medida, afastando qualquer possibilidade de atendimento a interesses pessoais ou privados." (STF, 2020).

> O Rio, dentro da realidade nacional, a gente está indo para cima. Só que o que causa uma tremenda preocupação é que, para tratar dessas novas relações sociais desenvolvidas, potencializadas pelo uso de tecnologia, a gente está muito atrás. A gente não tem o dado como um ativo organizacional (Delegado Civil 1).

Isso significa que, em sua visão, o potencial dos dados para fins de segurança pública é pouco ou mal explorado. Embora existam tecnologias capazes de operar *business analytics* baseadas nos dados, faltaria uma cultura que valorizasse esse potencial preditivo dos dados:

> O que a gente está tentando levar aqui no laboratório é pegar esses mesmos dados, só que todos os dados, olhar para trás para saber o que vai acontecer. *Isso se chama* business analytics*.* Você faz análise preditiva, que hoje isso é possível por causa da criação, do surgimento do fenômeno do big data e também do aumento do poder computacional, barateamento. A tecnologia mudou. Então hoje você faz armazenamento e processamento distribuído para analisar big data. *A gente não tem essa estrutura de processamento e armazenamento distribuído na polícia. Então, a gente não tem, e eu também não tenho, para fazer business analytics, eu preciso de cientista de dados*. Para montar essa infraestrutura de análise e processamento de armazenamento e processamento de big data, eu preciso de engenheiro de dados e as máquinas e o rádio. Eu não tenho engenheiro de dados e eu duvido que você vá em qualquer lugar na polícia e pergunte o que faz um engenheiro de dados. [...] *E aí a gente tem um problemaço. Por quê? O dado como ativo organizacional, ele é a matéria-prima para isso tudo* (Delegado Civil 1).

O potencial preditivo dos dados seria desperdiçado, portanto, em razão da falta de uma cultura de dados dentro das organizações, "[p]orque o que as pessoas, principalmente de umas gerações anteriores a nós, a minha, da minha geração para trás, as pessoas não entenderam que o dado é um ativo organizacional" (Delegado Civil 1). Essa perspectiva do dado como um ativo institucional, isto é, da tecnologia atrelada à perspectiva da instituição pública, é citada também pela interlocutora da polícia federal:

> Acho que temos que primar sempre pelo uso de tecnologias institucionais. Vai depender da organização da instituição, da possibilidade de poder fazer uso e estabelecer... vai ter dois caminhos na administração pública:

> […] então as áreas de tecnologia do Estado tem áreas que são muito fortes e desenvolvem tecnologias próprias para serem usadas na administração pública. Então eu acho isso, a gente tem que não ter resistência, mas buscar desenvolver tecnologias institucionais que possam fortalecer a gestão pública como um todo especialmente no sistema penal que estamos falando (Delegada Federal).

A mesma interlocutora segue pontuando que:

> A gente deve primar sempre pelas relações institucionais. Claro, o WhatsApp veio no Brasil principalmente e se usa muito indiscriminadamente. Quando eu mencionei que temos tecnologias que são institucionais, elas podem ser adquiridas, ter uma assinatura como a gente diz. Por exemplo, o Ministério da Justiça, ele usa todo o pacote da Microsoft para as interações, isso permite a interação. Eu sou totalmente a favor de usarmos as tecnologias institucionalizadas para poder manter essas relações justamente por isso. Você tá falando em nome da instituição, então tem que fazer de forma institucionalizada. Inclusive, a redelab que você falou, a gente tá construindo uma integração com ferramentas institucionalizadas para poder aumentar essa troca e poder fazer isso dentro de sistemas seguros (Delegada Federal).

No caso dessa fala, a interlocutora desloca a preocupação sobre a problemática de se ter ou não dados para a importância da legitimidade do uso das tecnologias de um ponto de vista institucional. É um debate relevante que retira do discurso de responsabilização apenas individual, do agente público, para a reflexão em torno do que concerne às instituições nesse debate sobre tecnologias. Nesse sentido, quando os atores mencionam a palavra "cultura" ou termos como "tecnologias institucionais" ou "ativo organizacional" compreendemos como uma tentativa de descentralizar o tema do aspecto dos indivíduos, numa reflexão que envolve o papel das instituições de segurança pública nesses processos de incorporação da tecnologia, inclusive em relação a um plano de desenvolvimento que precisa ocorrer de forma coerente no tempo e que deve ser assegurado pelos interesses da instituição, conforme destacam os interlocutores.

Tal pensamento fica expresso na fala do Policial Militar 7:

> O operador, lá na ponta, tem que entender, o gestor intermediário tem que entender, a cúpula da corporação tem que entender, tem que comprar ideia, *porque qualquer um desses caras que não tiver um plano de envolvimento*

> *nisso, se torna um elo fraco, que vai fragilizar exatamente esse desenvolvimento*. A ideia de que a tecnologia, a experiência que eu vi aqui e eu vi fora daqui, nacionalmente e internacionalmente, é que a tecnologia não substitui o homem, ela precisa ser parceira, ela precisa ser um braço, uma ampliação, uma onda à mão do homem. Então, não é só conscientizar, a tecnologia, também tem que ser a tecnologia que se ajuste, a ideia da customização, quer dizer, está ajustado com a realidade, e me arrisco a dizer, o preço, acho que a gente paga com relação ao uso da tecnologia. Entender, tudo que eu acabei de falar assim, é três coisas: o primeiro é entender que o erro faz parte, ele faz parte da tentativa, isso é padrão no método científico, não seria diferente da aplicação tecnológica, que é a aplicação da ciência, então o erro faz parte, é a necessidade de se identificar, aprender e procurar não cometer, é a pura essência da aprendizagem. *A segunda coisa é que a tecnologia pressupõe atualização constante*, então é alguma coisa que se "estartou" agora, já tem que se pensar se ano que vem continua tão bom quanto, se no outro ano já está na hora de se pensar em outra ferramenta, enfim, que possa ser utilizada (Policial Militar 7).

Uma fala do delegado da polícia civil é capaz de sintetizar a discussão travada neste tópico: "a gente na polícia, por falta de cultura, a gente trata muito mal o dado" (Delegado Civil 1). Assim, preocupação que desponta é como ocorrerá o tratamento dos dados, sobretudo no sentido de sua qualidade:

> A gente tem um poder, uma capacidade de coletar dados imenso. Mas se você coletar um dado que ele não tem um processo de governança, de qualidade, de gerenciamento do dado, do metadado, dos dados transacionais, dos dados gerenciais, você vai ter lixo. E você pode ter o melhor cientista de dados do mundo, mas se você der lixo para ele processar, ele vai processar no final e vai sair lixo (Delegado Civil 1).

Nesse sentido, vale mencionar o princípio da qualidade dos dados, que determina que os dados sejam objetivos, exatos e atualizados. Nos termos do art. 4º, inciso V, da LGPD,[39] esse princípio corresponde à "garantia, aos titulares, de

---

39 "A LGPD é o principal diploma legal brasileiro a dispor sobre o tratamento de dados pessoais. Todavia, conforme a determinação de seu art. 4º, inciso III, a Lei não se aplica ao tratamento de dados pessoais realizados para fins exclusivamente de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais. O objetivo dessa limitação é a suposta garantia do interesse público de combater infrações penais, crime organizado, fraudes digitais ou até mesmo terrorismo. Dessa forma, no âmbito do setor público, o uso de tecnologias de reconhecimento facial para os referidos fins encontra-se parcialmente

exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento" (LGPD, 2018). Para Frazão (2019), a fim de que haja um mínimo de confiança e tranquilidade quanto ao uso de algoritmos baseados em big data, são necessários dois tipos de controle referentes à qualidade dos dados. Primeiro, é necessário o controle sobre a qualidade dos dados em si, para verificar se atendem "aos requisitos da veracidade, exatidão, precisão, acurácia e sobretudo adequação e pertinência diante dos fins que justificam a sua utilização; segundo, deve-se avaliar "a qualidade do processamento de dados, a fim de saber se, mesmo a partir de dados de qualidade, a programação utilizada para o seu tratamento é idônea para assegurar resultados confiáveis" (Frazão, 2019).

Conclui-se que, a despeito do uso de tecnologias baseadas em dados (como bases de dados computadorizados) na previsão e repressão da criminalidade não ser uma exclusividade dos dias de hoje, há uma grande expectativa de que o big data expanda e acelere a capacidade das forças de segurança pública de descobrir e combater o crime (Joh, 2016).Tal expectativa se comprova nas falas de diferentes agentes de segurança pública entrevistados, acendendo o alerta para a necessidade de maior atenção quanto ao uso de big data no contexto de segurança pública no Brasil.

---

excepcionado do escopo de aplicação da LGPD. *Parcialmente excepcionado*, pois a inaplicabilidade da Lei nesses contextos não é absoluta. O art. 4º, em seu parágrafo primeiro, determina, além da necessidade de legislação específica para regulação das hipóteses do inciso III, que os princípios gerais de proteção ao titular de dados continuarão orientando qualquer esfera de tratamento, até mesmo em contextos de interesse público" (OLIVEIRA, 2021).

Considerações finais

Este relatório buscou sistematizar e analisar o resultado de dezoito meses de pesquisa sobre as estratégias de implementação das novas ferramentas tecnológicas no campo da segurança pública no Brasil, com pesquisa de campo na cidade do Rio de Janeiro. Assim, reunimos um quadro teórico que refletisse transversalmente sobre segurança pública e tecnologia. Unindo essas duas temáticas, apresentamos ao leitor um panorama nacional sobre o uso das ferramentas tecnológicas e, mais especificamente, promovemos uma escuta atenta dos agentes de segurança pública em relação ao que compreendem como tecnologia e aos empecilhos de sua implementação na cidade do Rio de Janeiro.

Dessa forma, explicamos que ao nos referirmos ao termo big data estamos falando sobre a análise de grandes quantidades de dados, realizada de maneira automatizada por algoritmos, com o intuito de extrair resultados e cumprir objetivos específicos. Fica claro em nossa pesquisa que tanto teóricos que se dedicam ao estudo da tecnologia quanto usuários e consumidores de tecnologia na área da segurança pública — aqui pensando nos agentes de segurança pública que entrevistamos — convergem no sentido de compreender que o big data é menos uma questão propriamente de dados, mas muito mais sobre a capacidade de pesquisa, agregação e referência cruzada de grandes conjuntos de dados. Esse paralelo em concordância não acontece à toa, demonstrando como o discurso dos especialistas em tecnologia está permeado no campo dos profissionais de segurança pública no Rio de Janeiro, local em que realizamos entrevistas em profundidade e a análise qualitativa de nossa pesquisa.

No capítulo dois, apresentamos os aspectos normativos que caracterizam a adoção de novas tecnologias para a persecução penal no Brasil e os desafios para o processo de regulação dos usos dentro de parâmetros jurídicos capazes de garantir o equilíbrio entre interesse público, redução da criminalidade e preservação das garantias individuais e direitos, a partir dos pilares constitucionais.

A partir disso, no capítulo três, optamos por contextualizar o leitor a partir de um panorama histórico do uso de tecnologias na segurança pública, tanto a nível nacional quanto, de forma mais detida, na cidade do Rio de Janeiro. Dessa forma, analisamos os Planos Nacionais de Segurança Pública e buscamos compreender os paradigmas envolvidos na política nacional voltada ao tema. Nesse contexto, os megaeventos se sobressaem como marco essencial para se pensar a adoção de tecnologias na área da segurança pública. No caso do Brasil, por

diversas razões, o legado dos megaeventos esteve relacionado à ampliação da segurança pública no combate à violência urbana.

Em seguida, no capítulo quatro, mapeamos as ferramentas tecnológicas a nível nacional. Diante da dificuldade de acesso às informações sobre o seu emprego pelos agentes de segurança pública, uma vez que o assunto é tratado como sigiloso pelas instituições, aplicamos análise documental sobre reportagens e publicações de grande circulação sobre o uso de tecnologias baseadas em dados pelas forças de segurança pública no Brasil. As tecnologias que foram citadas de maneira mais recorrente foram: câmeras corporais (*bodycams*), drones, reconhecimento facial e reconhecimento óptico de caracteres (OCR) para leitura de placas veiculares. Buscamos mapear todas as notícias existentes sobre o tema no Brasil dentro do critério temporal de primeiro de junho de 2021, data em que a pesquisa teve início, até 31 de maio de 2022. Nesse mesmo capítulo, optamos por realizar uma comparação mais específica entre os estados de São Paulo e Ceará.

Na segunda parte do relatório, enfocada na pesquisa empírica baseada em trabalho de campo junto a agentes de segurança pública, apresentamos a metodologia utilizada para a realização das entrevistas e a análise dos dados obtidos a partir delas. Com base nas falas de nossos interlocutores, isto é, de profissionais que atuam na área de segurança pública, principalmente no município do Rio de Janeiro, buscamos identificar categorias que nos fizessem compreender como as ferramentas tecnológicas têm sido incorporadas às rotinas de trabalho policial e judicial de persecução criminal.

Ao visitarmos as instituições e ao entrevistarmos os agentes de segurança pública, percebemos que as falas se concentraram em dois tópicos gerais: o interlocutor primeiramente definia o que considerava como tecnologia e, depois, elencava os empecilhos ou entraves à adesão das ferramentas tecnológicas. Assim, optamos por centrar nossa análise nesses dois aspectos. Destrinchamos, portanto, suas falas, como forma de compreender o que aqueles atores pensam sobre a adoção de tecnologias baseadas em dados no contexto da segurança pública e como percebem a utilização de novas ferramentas em sua rotina de trabalho: no policiamento ostensivo, na atividade investigativa e na persecução penal.

É possível notar a inclinação dos atores em direção à inovação. Isso é particularmente verdade para aqueles que ocupam cargos “de alto escalão” ou

gerência, que enxergam nas novas tecnologias um aliado ao combate à criminalidade, conferindo maior eficiência no trabalho policial. Quanto àqueles "da ponta", isto é, agentes de segurança pública que realizam o trabalho cotidiano, nas ruas, é possível identificar certa resistência, ora por desconhecimento quanto ao funcionamento das novas tecnologias em si, ora pelo receio de "ser vigiado" e, eventualmente, "punido".

Há também consenso no sentido de que não basta a aquisição de novos equipamentos sem que se tenha, concomitantemente, o fomento à utilização das novas tecnologias por parte dos agentes, o que implica uma necessidade de treinamento e capacitação, por vezes impossibilitada pela ausência de recursos dentro das instituições. Esse aspecto, já parte do senso comum e do discurso político no Brasil, é ressaltado por diversos dos entrevistados como um entrave à modernização e digitalização das forças de segurança pública no país. Faltaria, para além de uma "cultura de dados" dentro das organizações, um interesse político em implementar e/ou dar continuidade a projetos que "não dariam resultados de uma noite para a outra", como ressaltado por um dos delegados civis entrevistados. As exceções mencionadas referem-se, ainda que com ressalvas, ao caso da polícia rodoviária federal e ao estado do Ceará, que contam com um maior desenvolvimento tecnológico atribuído tanto à mudança de mentalidade a nível institucional (uma alternativa à "falta de recursos" enfrentada pela instituição) quanto ao investimento em desenvolvimento e pesquisas junto à academia no estado nordestino.

Chamou-nos atenção, igualmente, a recorrência com que a questão da integração entre bases de dados é mencionada. Diversos atores, principalmente aqueles da polícia militar, apontam que o acesso às bases de dados sob domínio de outras instituições de segurança pública seria essencial para a melhoria da prestação de seus serviços, mas que tal compartilhamento não ocorreria de maneira satisfatória. Conforme se extrai das falas dos entrevistados, a falta de integração não seria um problema apenas interinstitucional, mas também dentro da mesma instituição, uma vez que diferentes estados não compartilhariam de um sistema unificado de armazenamento e acesso a dados.

A análise documental das reportagens e publicações oficiais levantadas ao longo dos últimos dezoito meses, somada à análise qualitativa das entrevistas, permite concluir que, no Brasil, há iniciativas majoritariamente isoladas de implementação de tecnologias baseadas em dados no contexto da segurança pública. O discurso de que, no país, não se investe em tecnologia

para combate à criminalidade não se sustenta, uma vez que pudemos observar diferentes tentativas de se implementar inovações, como câmeras com reconhecimento facial, drones, leitores OCR e até mesmo técnicas de policiamento preditivo. O que ocorre, como constatamos, é que os frequentes *trade-offs* com que as instituições se deparam não permitem que, na maior parte das vezes, implementem-se inovações tecnológicas da maneira que seus agentes consideram ideal.

O contexto político que se apresenta atualmente é de escalação de três ministérios no novo governo federal para promover a redução dos índices de mortes: Justiça e Segurança Pública, Igualdade Racial e Direitos Humanos. Sobretudo em matéria de diminuição da letalidade policial e de pessoas negras, que sofrem a maior parte das abordagens policiais e são parcela majoritária da população carcerária no Brasil (Nunes, 2022). Pretos e pardos somam 77,6% das mortes por causas violentas, um número muito discrepante quando comparado aos 21,7% de vítimas brancas. Do total de mortes violentas em 2022, o último anuário brasileiro de segurança pública aponta que 12,9% aconteceram em ações policiais.

Estes dados não servem como forma de desautorizar o direito, o Estado ou as forças de segurança no combate à violência, mas como forma de reposicionar o papel das tecnologias neste cenário. Esses dados têm sido produzidos por décadas de racismo e violência contra a população negra e comporão esse grande conjunto de dados que denominamos big data.

As informações de que carecem as forças de segurança para uma efetiva atuação no combate à criminalidade não são neutras, e sim reproduções de processos históricos de repressão e violência de contornos políticos, econômicos, sociais e jurídicos. A partir desses os dados, caso não seja realizada uma leitura atenta dos processos de aplicação de determinados aparatos tecnológicos e em contextos específicos, os sistemas automatizados aprenderão e reproduzirão modelos enviesados e discriminatórios, reforçando estereótipos e violências presentes na sociedade e que serão utilizados para predição de crimes, processamento de imagens, reconhecimento de padrões faciais e toda sorte de aplicações tecnológicas.

Muitas propostas têm ganhado corpo no Brasil: incentivo e uso de câmeras em carros e fardas policiais, adoção de tecnologias de reconhecimento facial, treinamento de agentes para utilizar tecnologias complexas como drones, *analytics*

de big data e outras. No entanto, é necessário cautela para que estes aparatos tecnológicos não sejam subvertidos em ferramentas de perpetuação da desigualdade e da violência.

As novas tecnologias têm demonstrado ser instrumentos relevantes na redução da criminalidade e letalidade policial. Para tanto, seus usos dependem de apoio à capacitação e à formação dos agentes e do uso de instrumentos que impeçam o uso abusivo da força. É muito importante reconhecer que as tecnologias de big data possuem relevantes usos, mas tão importante quanto, é considerar seus potenciais desusos. Sobretudo se as mesmas tecnologias prometem avanços que acabam por se desdobrar em retrocessos, principalmente para grupos étnicos, sociais e politicamente minoritários.

Referências bibliográficas

ALVES, Nubia. Prefeitura lança Sistema de reconhecimento facial nas escolas e Cmeis de Goiânia. **Prefeitura de Goiânia**. 26 out. 2021. Disponível em: <https://www.goiania.go.gov.br/prefeitura-lanca-sistema-de-reconhecimento-facial-nas-escolas-e-cmeis-de-goiania/> Acesso em: 07 ago. 2022.

ALVES, Priscila Mello. **Inteligência artificial e redes neurais**. Centro de Pesquisa em Ciência, Tecnologia e Sociedade. Ipea, 11 jun. 2020. Disponível em: <https://www.ipea.gov.br/cts/pt/central-de-conteudo/artigos/artigos/106-inteligencia-artificial-e-redes-neurais>. Acesso em: 23 jan. 2023.

ALVES, Tatiana. PM do Rio vai usar drones para segurança do Reveillón em Copacabana. Rio de Janeiro: Rádio Agência Nacional, 23 dez. 2022. Disponível em: <https://agenciabrasil.ebc.com.br/radioagencia-nacional/geral/audio/2022-12/pm-do-rio-vai-usar-drones-para-seguranca-do-reveillon-em-copacabana>. Acesso em: 26 jan. 2023.

AMARAL, Thiago Bottino do et al. **Os desafios da integração na segurança pública no estado do Rio de Janeiro**. Rio de Janeiro: FGV Direito Rio, 2020.

ARNAUDO, Daniel; MONACO, Nick. NATIONAL DEMOCRATIC INSTITUTE. **Análise de dados para o monitoramento de redes sociais**. Tutorial sobre Técnicas, Ferramentas e Metodologias de Monitoramento e Análise de Redes Sociais. [Ss.l.]: National Democratic Institute, maio 2020. Disponível em: https://www.ndi.org/sites/default/files/247805_NDI_Social%20Media%20Monitoring%20Guide_Portuguese.pdf. Acesso em: 20 jul. 2022.

ARRUDA, A. J. P.; RESENDE, A. P. B. A.; FERNANDES, F. A. SISTEMAS DE POLICIAMENTO PREDITIVO E AFETAÇÃO DE DIREITOS HUMANOS À LUZ DA CRIMINOLOGIA CRÍTICA. **Direito Público**, *[S. l.]*, v. 18, n. 100, 2021. DOI: 10.11117/rdp.v18i100.5978. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5978. Acesso em: 25 jan. 2023.

AZEVEDO, Cynthia Picolo Gonzaga de; LIMA, Eliz Marina Bariviera de; SILVA, Felipe Rocha da; RODRIGUES, Gustavo Ramos; DUTRA, Luiza Corrêa de Magalhães; SANTARÉM, Paulo Renáda Silva; VIEIRA, Victor Barbieri Rodrigues. **Nota técnica**: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022. Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), novembro de 2022. Disponível em:<https://irisbh.com.br/wp-content/uploads/2022/11/Nota-tecnica-Analise-comparativa-entre-o-anteprojeto-de-LGPD-Penal-e-o-PL-1515-2022.pdf>. Acesso em: 24 jan 2023.

AZEVEDO, Felipe. Câmara derruba reconhecimento facial e aprova instalação de câmeras de segurança em Fortaleza. Fortaleza: **Diário do Nordeste**, 03 nov. 2022. Disponível em: <https://diariodonordeste.verdesmares.com.br/pontopoder/camara-derruba-reconhecimento-facial-e-aprova-instalacao-de-cameras-de-seguranca-em-fortaleza-1.3296590>. Acesso em: 26 jan. 2023

BACHNER, Jennifer. **Predictive policing: preventing crime with data and analytics. John Hopkins University**. IBM Center for the Business of Government. Improving Performance Series, 2013. Disponível em: <https://www.businessofgovernment.org/sites/default/files/Predictive%20Policing.pdf>. Acesso em: 07 ago. 2022.

BANDEIRA, Beatriz. Elmano fala em implementar tecnologia de reconhecimento facial no Ceará. Fortaleza: **O Povo**, 04 out. 2022. Disponível em: <https://www.opovo.com.br/noticias/ceara/2022/10/04/elmano-fala-em-implementar-tecnologia-de-reconhecimento-facial-no-ceara.html>. Acesso em: 26 jan. 2023.

BARBOZA, Anderson Duarte. Prevenção e repressão aos crimes vinculados ao uso de veículos: tecnologias e estratégias de melhoria da segurança pública em estados brasileiros. **Revista Susp Brasília**, v. 1, n. 2, p. 42-65, jul./dez. 2022.

BARBROOK, Richard; CAMERON, Andy. The California Ideology. **Net,** Londres, 2000. The Hypermedia Research Centre. Disponível em: <http://www.hrc.wmin.ac.uk/theory-californianideology-main.html>. Acesso em: 04 ago. 2022.

BELL, Daniel. **O advento da sociedade pós-industrial**. Tradução de Heloysa de Lima Dantas. São Paulo: Ed. Cultrix, 1974.

BOYD, Danah; CRAWFORD, Kate. "Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon". **Information, Communication & Society** 15.5 (2012): 662-679.

BRASIL, Janine. Câmeras com tecnologia de reconhecimento facial vão ser instaladas em Rio Branco. **G1**. Acre. 14 fev. 2022. Disponível em: <https://g1.globo.com/ac/acre/noticia/2022/02/14/cameras-com-tecnologia-de-reconhecimento-facial-vao-ser-instaladas-em-rio-branco.ghtml>. Acesso em: 06 ago. 2022.

Broadband Commission. **The State of Broadband: Broadband catalyzing sustainable development**. United Nations: Geneva, Switzerland (2016). Disponível em: <https://www.broadbandcommission.org/Documents/reports/bb-annualreport2016.pdf>. Acesso em: 13 jun. 2023.

CAI, Yijun; LI, Dian; WANG, Yuyue. **Intelligent Crime Prevention and Control Big Data Analysis System Based on Imaging and Capsule Network Model. Neural Processing Letters**. Springer Nature, 30 abr. 2020. Disponível em: <https://link.springer.com/article/10.1007/s11063-020-10256-1>. Acesso em: 05 ago. 2022.

CÂMERA no uniforme será usada por PMs do Rj a partir de segunda-feira. Rio de Janeiro: **RJ2**. G1, 28 maio 2022. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2022/05/28/pms-do-rj-vao-comecar-a-usar-cameras-corporais-na-segunda-feira-diz-porta-voz.ghtml>. Acesso em: 26 jan 2023.

CARDEAL, Camila Costa; RIBEIRO, Ludmila Mendonça Lopes. Relações de gênero nas Guardas Municipais. **Revista Brasileira de Segurança Pública**, v. 11, n. 1, 2017.

CARDOSO, Bruno. A lógica gerencial-militarizada e a segurança pública no Rio de Janeiro: O CICC-RJ e as tecnologias de (re)construção do Estado. **Dilemas**, Rev. Estud. Conflito e Controle Soc., Rio de Janeiro, edição especial n. 3, 2019.

CARDOSO, Bruno de Vasconcelos. Megaeventos esportivos e modernização tecnológica: planos e discursos sobre o legado em segurança pública. **Horizontes Antropológicos**, v. 19, p. 119-148, 2013.

CASTELLS, Manuel. **A sociedade em rede**. Volume I. 6. ed. Tradução de Roneide Venancio Majer. São Paulo: Paz e Terra, 2011.

_____. **Ruptura**: a crise da democracia liberal. Trad. Joana Angelica d'Ávila Melo. Rio de Janeiro: Zahar, 2018.

CHEN T. et al. **National governance in the age of big data**. China Social Science Press, Beijing, p. 103. Tu Z (2014) The data: the big data revolution, history, reality and future, vol 27. CITIC Publishing House, Beijing, pp 258-259.

COALIZÃO Direitos na Rede. **Reforma do Código de Processo Penal pode aumentar vigilância e precisa de equilíbrio em questões de tecnologia**. 20 maio 2021. Disponível em: <https://direitosnarede.org.br/2021/05/20/reforma-do-codigo-de-processo-penal-pode-aumentar-vigilancia-e-precisa-de-equilibrio-em-questoes-de-tecnologia/>. Acesso em: 25 jan. 2023.

COSTA, Eduarda; REIS, Carolina. Histórico da LGPD Penal: o que foi feito até aqui e quais são os próximos passos? Privacidade e Proteção de Dados. **Lapin**. Blog. 16 abr. 2021. Disponível em: <https://lapin.org.br/2021/04/16/lgpd-penal-o-que-foi-feito-ate-aqui-e-quais-sao-os-proximos-passos/>. Acesso em: 24 jan. 2023.

CRUZ, Elaine Patricia. Câmeras corporais continuarão a ser utilizadas pela PM em São Paulo. São Paulo: **Agência Brasil**, 05 jan. 2023. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2023-01/cameras-corporais-continuarao-ser-utilizadas-pela-pm-em-sao-paulo>. Acesso em: 26 jan. 2023

CRUZ, Elaine Patricia. TJ mantém proibição de câmeras de reconhecimento facial no metrô de SP. São Paulo: **Agência Brasil**, 18 abr. 2022. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2022-04/tj-mantem-proibicao-de-cameras-de-reconhecimento-facial-no-metro-de-sp>. Acesso em: 08 ago. 2022.

DELGADO, Letícia. **Formação da agenda municipal de políticas públicas de segurança**: a emergência das políticas e dos dispositivos de Segurança Pública em Juiz de Fora/MG. Tese de Doutorado. PPGSD, Niterói, 2021.

DIAS, Tatiana; HVISTENDAHL, Mara. Polícia do Rio comprou tecnologia da Oracle usada por países autoritários. The Intercept Brasil, 10 mar. 2021. Disponível em: <https://theintercept.com/2021/03/10/policia-rio-tecnologia-oracle-policias-paises-autoritarios/>. Acesso em: 21 jan. 2023

DIETER, Mauricio. Big data e devido processo: poder penal preditivo. In: BRITO, Francisco; SIMÃO, Barbara (org.). **Direitos fundamentais e processo penal na era digital**. Doutrina e prática em debate 4. 1. ed. São Paulo: Internet Lab, 2021.

_____. Política Criminal Atuarial: a criminologia do fim da história. 2012. 309 f. **Tese** (Doutorado em Direito) — Universidade Federal do Paraná, Curitiba, 2012.

ELANDER, Bruno. Ruas de Manaus têm câmeras com reconhecimento facial e de placas; até o final do ano serão 180. **Rio Mar FM**. 12 abr 2021. Disponível em: <https://radioriomarfm.com.br/ruas-de-manaus-tem-cameras-com-reconhecimento-facial-e-identificacao-de-placas-ate-o-final-do-ano-serao-180/>. Acesso em: 06 ago. 2022.

FERREIRA, Paula; BANDEIRA, Karolini; SCHMITT, Gustavo; ALFANO, Bruno. Para reduzir morte de jovens negros governo quer ampliar uso de câmeras em policiais, medida já adotada em 12 estados. Rio de Janeiro: **Extra**, 06 jan. 2023. Disponível em: <https://extra.globo.com/noticias/brasil/para-reduzir-mortes-de-jovens-negros-governo-quer-ampliar-uso-de-cameras-em-policiais-medida-ja-adotada-em-12-estados-25639560.html>. Acesso em: 26 jan. 2023.

FORUM brasileiro de segurança pública. Anuário brasileiro de segurança pública 2022. Ano 16, 2022. Disponível em: <https://forumseguranca.org.br/wp-content/uploads/2022/06/anuario-2022.pdf?v=5>. Acesso em: 26 jan. 2023.

FRAGOSO, Suely; RECUERO, Raquel; AMARAL, Adriana. **Métodos de pesquisa para internet**. Porto Alegre: Sulina, 2011.

FRAZÃO, Ana. "Fundamentos da proteção de dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados". In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 1.ed. São Paulo: Thomson Reuters Brasil, 2019. p. 23-52.

FRAZÃO, Ana. "Fundamentos para a proteção dos dados pessoais. Noções introdutórias para a compreensão da LGPD". In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). **A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Revista dos Tribunais, 2019.

FREIRE, Moema. Paradigmas de segurança no Brasil: da ditadura aos nossos dias. **Revista Brasileira de Segurança Pública**. Ano 3, edição 5, Ago/Set, 2009.

GERALDO, Pedro Heitor Barros; FONTAINHA, Fernando de Castro. "Por uma sociologia empírica do Direito". In: FONTAINHA, Fernando de Castro; GERALDO, Pedro Heitor Barros (orgs.). **Sociologia empírica do Direito**. Lisboa: Juruá, 2015, p. 9-20.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

GOES, Ancelmo. Estado do Rio compra 35 drones e quer criar gestão operacional inédita no Brasil. Rio de Janeiro: **O Globo**, 15 ago 2022. Disponível em: <https://oglobo.globo.com/blogs/ancelmo-gois/coluna/2022/08/estado-do-rio-compra-35-drones-e-quer-criar-gestao-operacional-inedita-no-brasil.ghtml>. Acesso em: 26 jan 2023.

GOMES, Rodrigo Dias de Pinho. **Big data**: desafios à tutela a pessoa humana na sociedade da informação. Rio de Janeiro: Lumen Juris, 2019.

GOODFELLOW, Ian *et al*. **Deep learning**. Vol. 1. Cambridge: MIT press, 2016

GONÇALVES, Eliane. São Paulo: quase todos os indicadores de violência pioraram em 2022. São Paulo: **Rádio Agência Nacional**, 26 abr. 2022. Disponível em: <https://agenciabrasil.ebc.com.br/radioagencia-nacional/seguranca/audio/2022-04/sao-paulo-quase-todos-indicadores-de-violencia-pioraram-em-marco>. Acesso em: 07 ago. 2022.

GRAVES, Alex, ABDEL-RAHMAN, Mohamed. Speech recognition with deep recurrent neural networks. **Acoustics, speech and signal processing (icassp)**, 2013 ieee international conference, IEEE, 2013

HARCOURT, Bernard E. **Against Prediction**: profiling, policing and punishing in an Actuarial Age. Chicago (Illinois): The University of Chicago Press, 2007.

HARTMANN, Ivar A. *et al*. **Big data e gestão processual**. 2015, Rio de Janeiro: FGV Direito Rio. Disponível em: <https://bibliotecadigital.fgv.br/dspace/handle/10438/15167>. Acesso em: 05 ago. 2022.

HERRERO, Dirceu. Prefeitura apresenta sistema de segurança com reconhecimento facial na Expoingá. Maringá: **Site da Prefeitura de Maringá**, 13 maio 2022. Disponível em: <http://www.maringa.pr.gov.br/site/noticias/2022/05/13/prefeitura-apresenta-sistema-de-seguranca-com-reconhecimento-facial-na-expoinga/39806>. Acesso em: 13 maio 2022.

INTERNATIONAL TELECOMMUNICATION UNION. **Measuring the information society report**. UN, 2017. Disponível em: <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf>. Acesso em: 05 ago. 2022.

JOH, Elizabeth E. The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing. **Harvard Law & Policy Review**, vol. 10, 2016.

KANT DE LIMA, Roberto; EILBAUM, Lucia; PIRES, Lenin dos Santos. **Construção da verdade e a administração dos conflitos no Rio de Janeiro**: um olhar sobre as reformas das instituições judiciárias e policiais, p. 1-22, 2010.

KOPITKKE, Alberto Winogron. A (in) capacidade insitucional do Governo Federal na Segurança Pública. **Boletim de Análise Político-Institucional**, n. 11, jan-jun, 2017. Disponível em: <BAPI_n11_ Incapacidade.pdf (ipea.gov.br)>. Acesso em 24 de jul. 2022.

KOVACS, Leandro. O que é OCR? [OpticalCharacterRecognition] São Paulo: **Tecnoblog**, 2022. Disponível em: <https://tecnoblog.net/responde/o-que-e-ocr-optical-character-recognition/>. Acesso em: 07 ago. 2022.

KREMER, Bianca. **Direito e tecnologia em perspectiva americana:** autonomia, algoritmos e vieses raciais. 2021. 299 f. Tese (Doutorado em Direito) — Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2021.

LIMA, Roberto Kant de; BAPTISTA, Bárbara Gomes Lupetti Baptista. "Como a Antropologia pode contribuir para a pesquisa jurídica? Um desafio metodológico" **Anuário Antropológico** 39.1 (2014): 9-37.

LIMA, Thallita Gabriele Lopes. **Câmeras corporais** [livro eletrônico] / Thallita Gabriele Lopes Lima, Pablo Nunes, Thaís Gonçalves Cruz. — Rio de Janeiro: CESeC, 2022. Disponível em: <https://opanoptico.com.br/panoptico-lanca-o-fasciculo-de-estreia-da-colecao-panorama-sobre-as-cameras-corporais-e-sua-utilizacao-na-seguranca-publica/>. Acesso em: 26 jan. 2023.

MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018.

MARIANO, Marcelo. Goiás está fora do movimento parlamentar contra reconhecimento facial em espaços públicos. **Diário de Goiás**. Vigilância. 19 jun. 2022. Disponível em: <https://diariodegoias.com.br/goias-esta-fora-de-movimento-parlamentar-contra-reconhecimento-facial-em-espacos-publicos/>. Acesso em: 07 ago. 2022.

MATHIAS, Suzeley; ZAGUE, Jose Augusto; SANTOS, Leandro Fernandes. A política militar brasileira no governo Dilma Rousseff: o discurso e a ação. **Opinião Pública**, Revista do CEOP, Campinas, vol. 25, n. 1, jan-abr., p. 136-168, 2019.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data: A revolution that will transform how we live, work, and think**. Boston: Houghton Mifflin Harcourt, 2013.

MELLO, Daniel. Câmeras corporais reduzem em 87% número de confrontos da PM em SP. São Paulo: **Agência Brasil**, 11 abr. 2022. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2022-04/cameras-corporais-reduzem-em-87-numero-de-confrontos-da-pm-de-sp>. Acesso em: 08 ago. 2022.

MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. Dissertação (Mestrado em Direito) — Faculdade de Direito da Universidade de Brasília. Brasília [DF], 2008.

_____. **Democracia, poder informacional e vigilância**. Fumus Boni Iuris. O Globo. 13 ago. 2022. Disponível em: <https://oglobo.globo.com/blogs/fumus-boni-iuris/post/2022/08/laura-schertel-democracia-poder-informacional-e-vigilancia.ghtml>. Acesso em: 20 out. 2022.

MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. **RJLB**, vol. 5, n.1, 2019.

MONTEIRO, Joana; FAGUNDES, Eduardo; GUERRA, Julia; PIQUET, Leandro. **Avaliação do impacto das câmeras corporais pela Policia Militar do Estado de São Paulo**. Out. 2022. São Paulo: CCAS — FGV SP, 2022. Disponível em: <https://ccas.fgv.br/sites/default/files/projetos/ccas_relatorio_de_pesquisa_cameraspmesp_0.pdf>. Acesso em: 26 jan. 2023.

MORAES, Felipe de. **Policiamento preditivo e aspectos constitucionais**. Belo Horizonte: Dialética, 2022.

MULHOLLAND, Caitlin; FRAJHOF, Isabela. Prefácio. **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago, 2020.

NATIONAL DEMOCRATIC INSTITUTE. **Análise de dados para o monitoramento de redes sociais**. Tutorial sobre técnicas, ferramentas e metodologias de monitoramento e análise de redes sociais. [*s.l.*], maio 2020. Disponível em: <https://www.ndi.org/sites/default/files/247805_NDI_Social%20Media%20Monitoring%20Guide_Portuguese.pdf>. Acesso em: 20 jul. 2022.

OLIVEIRA JUNIOR, Almir. "Dá para confiar nas polícias? Confiança e percepção social da polícia no Brasil". **Revista Brasileira de Segurança Pública**, [S. l.], v. 5, n. 2, 2011. Disponível em: <https://revista.forumseguranca.org.br/index.php/rbsp/article/view/94>. Acesso em: 13 jun. 2023.

OLIVEIRA, Samuel R. **Sorria, você está sendo filmado**. Repensando Direitos na Era do Reconhecimento Facial. São Paulo: Thomson Reuteurs, 2021.

PAIVA, Fernando. Polícia civil em São Paulo usará reconhecimento facial em investigações. São Paulo: **Mobile Time**, 11 nov. 2019. Disponível em: <https://www.mobiletime.com.br/noticias/11/11/2019/policia-civil-de-sao-paulo-usara-reconhecimento-facial-em-investigacoes/>. Acesso em: 08 ago. 2022.

PEDERZOLI, Cecilia. **Reconhecimento facial já cadastrou mais de 7 mil sentenciados em Minas**. Minas Gerais: Diário do Aço, 2019. Disponível em: <https://www.diariodoaco.com.br/noticia/0071561-reconhecimento-facial-ja-cadastrou-mais-de-7-mil-sentenciados-em-minas>. Acesso em: 07 ago. 2022.

PEDREZANI, Thiago. Segurança Pública de São Paulo ingressa na era dos drones e da vigilância antidrone. São Paulo: **Drone Operacional**, 6 dez. 2019. Disponível em: <https://www.resgateaeromedico.com.br/seguranca-publica-de-sao-paulo-ingressa-na-era-dos-drones-e-da-vigilancia-antidrone/>. Acesso em: 08 ago. 2022.

PETROCILO, Carlos; LACERDA, Lucas; SETO, Guilherme. Prefeitura revê, mas não desiste de programa de reconhecimento facial em SP. Tecnologia. São Paulo: **Folha de São Paulo**, 2 dez 2022. Disponível em: <https://www1.folha.uol.com.br/cotidiano/2022/12/suspenso-apos-criticas-projeto-de-reconhecimento-facial-sera-mantido-diz-nunes.shtml>. Acesso em: 26 jan. 2023.

PM do Amazonas desenvolve tecnologia de reconhecimento facial de foragidos pelo celular. **Informe Amazonas**. 17 nov. 2021. Disponível em: <https://informeamazonas.com.br/pm-do-amazonas-desenvolve-tecnologia-de-reconhecimento-facial-de-foragidos-pelo-celular/> Acesso em: 06 ago. 2022.

QUAN-HAASE, Anabel; WELLMAN, Barry. Hyperconnected net work: computer-mediated community in a high-tech organization. In: **The firm as a collaborative community***:* reconstructing trust in the knowledge economy. Oxford: Oxford University Press, 2006, p. 281-333, 2006.

RAMIRO, Andre; PEREIRA, Ana Barbara Gomes; ROGRIGUES, Gustavo Ramos; AMARAL, Pedro; VIEIRA, Victor Barbieri Rodrigues. **Decálogo de recomendações sobre direitos digitais e produção de provas**. 2021. Disponível em: <https://irisbh.com.br/wp-content/uploads/2021/08/Decalogo-de-recomendacoes-sobre-direitos-digitais-e-producao-de-provas-IRIS-IPREC-CDR.pdf>. Acesso em: 25 jan. 2023.

REFORMA do Código de Processo Penal pode aumentar vigilância e precisa de equilíbrio em questões de tecnologia. **Coalizão Direitos na Rede**, Brasília: mai. 2021. Disponível em: <https://direitosnarede.org.br/2021/05/20/reforma-do-codigo-de-processo-penal-pode-aumentar-vigilancia-e-precisa-de-equilibrio-em-questoes-de-tecnologia/>. Acesso em: 25 jan. 2023.

RORAIMA instala câmeras de monitoramento na fronteira do Brasil com a Venezuela. **Segurança eletrônica**, 2022. Disponível em: <https://revistasegurancaeletronica.com.br/roraima-instala-cameras-de-monitoramento-na-fronteira-do-brasil-com-a-venezuela/>. Acesso em: 06 ago. 2022.

SAISSE, Renan. Big Data contra o crime: efeito minority report.Revista. **Digital Direito & TI**, [s. l.], 7 set. 2017. Disponível em: <https://www.direitoeti.com.br/direitoeti/article/download/79/77>. Acesso em: 26 jan. 2023.

SCHENDES, William. SmartSampa: projeto de reconhecimento facial em SP será investigado por inquérito. Segurança e privacidade. **Olhar digital**. 18 jan. 2023. Disponível em: <https://olhardigital.com.br/2023/01/18/seguranca/smart-sampa-projeto-de-reconhecimento-facial-em-sp-sera-investigado-por-inquerito/>. Acesso em: 26 jan. 2023

SCHMIDT, Flávia de Holanda. **Presença de militares em cargos e funções comissionados do executivo federal**. IPEA. Nota técnica. Brasília, 2022. Disponível em: <https://www.ipea.gov.br/portal/images/stories/PDFs/pubpreliminar/220530_publicacao_preliminar_presenca_de_militares_em_cargos_novo.pdf>. Acesso em: 24 jul. 2022.

Seap lança sistema de reconhecimento facial para segurança no sistema penitenciário. **O Impacto**. 28 jan. 2022. Disponível em: <https://oimpacto.com.br/2022/01/28/2seap-lanca-sistema-de-reconhecimento-facial-para-seguranca-no-sistema-penitenciario/>. Acesso em: 06 ago. 2022.

SEGAL, Howard P. **Technological utopianism in American culture**. 20th Anniversary Ed. First Syracuse University Press Edition: 2005.

SERBENA, Cesar A. Interfaces atuais entre a E-Justiça e a Q-Justiça no Brasil. **Revista de Sociologia e Política**. v. 21, n. 45, pp. 47-56, 2013. Disponível em: https://doi.org/10.1590/S0104-44782013000100005. Acesso em: 20 jul. 2022.

SESTREM, Gabriel. Ao STF as polícias do Rio de Janeiro se posicionam contra o uso de câmeras em agentes de forças especiais. Rio de Janeiro: **Gazeta do Povo**, 02 jan 2023. Disponível em: <https://www.gazetadopovo.com.br/vida-e-cidadania/ao-stf-policias-rj-se-posicionam-contra-uso-cameras-agentes-forcas-especiais/>. Acesso em: 26 jan 2022.

SILVA, Fabio de Sá e. Barcos contra a corrente: a Política Nacional de Segurança Pública de Dilma Rousseff a Michel Temer. **Boletim de Análise Político-Institucional**, n. 11, jan-jun, 2017. Disponível em: <BAPI_n11_Barcos.pdf (ipea.gov.br)>. Acesso em: 23 jul. 2022.

SOARES, Luiz Eduardo. A Política Nacional de Segurança Pública: histórico, dilemas e perspectivas. **Estudos Avançados** [online]. 2007, v. 21, n. 61 [Acessado 24 Maio 2022], pp. 77-97. Disponível em: <https://doi.org/10.1590/S0103-40142007000300006>. Epub 11 Jun 2008. ISSN 1806-9592. https://doi.org/10.1590/S0103-40142007000300006.

SOUZA, Luís Antônio Francisco de; SERRA, Carlos Henrique Aguiar. Quando o Estado de exceção se torna permanente: reflexões sobre a militarização da segurança pública no Brasil. **Tempo Social** [online]. 2020, v. 32, n. 2 [Acessado 25 Julho 2022] , pp. 205-227. Disponível em: <https://doi.org/10.11606/0103-2070.ts.2020.158668>. Epub 17 Ago 2020. ISSN 1809-4554. https://doi.org/10.11606/0103-2070.ts.2020.158668.

SPANIOL, Maria Inês; JÚNIOR, Martim Cabeleira Moraes; RODRIGUES, Carlos Roberto Guimarães. Como tem sido planejada a segurança pública no Brasil? Análise dos Planos e Programas Nacionais de Segurança implantados no período pós-Redemocratização. **Revista Brasileira de Segurança Pública**, v. 14, n. 2, p. 100-127, São Paulo, ago/set de 2020.

STURGILL, Kristi. **Santa Cruz becomes the first U.S. city to ban predictive policing**. 2020, Los Angeles: Los Angeles Times. 26 jun. 2020. Disponível em: <https://www.latimes.com/california/story/2020-06-26/santa-cruz-becomes-first-u-s-city-to-ban-predictive-policing>. Acesso em: 05 ago. 2022.

TOURAINE, Alain. **The post-industrial society**: tomorrow's social history — classes, conflict and culture in the programmed society. Translated by Leonard F. X. Mayhew. New York. Random House, 1971.

TYLER, T. R. Enhancing police legitimacy. **The Annals of the American Academy of Political and Social Science**, v. 593, p. 84-99, 2004.

WOLTER, Jürgen. **O inviolável e o intovável no direito processual penal**: reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. Trad. Luis Greco; Alaor Leite; Eduardo Viana. 1. ed. São Paulo: Marcial Pons, 2018.

VIANA, Eduardo; MONTENEGRO, Lucas; ORLANDINO, Gleizer. **A esfera protegida dos dados pessoais e as intervenções informacionais do Estado**: A dogmática constitucional aplicada ao tratamento de dados na Segurança Pública e no Processo Penal. **Relatório de Consulta**, 2020. Disponível em: <https://www.academia.edu/45293835/A_esfera_protegida_dos_dados_pessoais_e_as_interven%C3%A7%C3%B5es_informacionais_do_Estado_A_dogm%C3%A1tica_constitucional_aplicada_ao_tratamento_de_dados_na_Seguran%C3%A7a_P%C3%BAblica_e_no_Processo_Penal>. Acesso em: 05 ago. 2022.

ZAMBARDA, Pedro. **Internet das coisas**: entenda o conceito e o que muda com a tecnologia. Techtudo. 16 ago 2014. Disponível em: <https://www.techtudo.com.br/noticias/noticia/2014/08/internet-das-coisas-entenda-o-conceito-e-o-que-muda-com-tecnologia.html>. Acesso em 05 ago. 2022.

ZUBOFF, Shoshana. **Big Other**: surveillance capitalismo and the prospects of an information civilization. Journal of Information Technology, v.30, 2015.

_____. You are now remotely controlled: surveillance capitalists control the science and the scientists, the secrets and the truth. **New York Times**. Opinion. 24 Jan. 2020. Disponível em: <https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html>. Acesso em 04 ago. 2022.

Coordenadores

Thiago Bottino

Doutor e mestre em Direito pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio). Pós-doutorado pela Columbia Law School. Professor da FGV Direito Rio.

Daniel Vargas

Doutor e mestre em Direito pela Harvard Law School. Professor da FGV Direito Rio.

Fernanda Prates

Doutora em Criminologia pela Universidade de Montreal. Pós-doutora em Direito pela Fundação Getulio Vargas (FGV). Professora da FGV Direito Rio.

Pesquisadores

Bianca Kremer

Doutora em Direito pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio). Mestre em Direito Constitucional pela Universidade Federal Fluminense (UFF).

Victoria de Castro Pires

Doutoranda pelo Programa de Pós-graduação em Sociologia e Antropologia da Universidade Federal do Rio de Janeiro (UFRJ). Mestre em Ciências Jurídicas e Sociais pela Universidade Federal Fluminense (UFF).

Samuel Rodrigues de Oliveira

Doutorando pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio). Mestre em Direito e Inovação pela Universidade Federal de Juiz de Fora (UFJF).

Lucas Krause

Mestre em Direito pela Universidade Federal do Rio de Janeiro (UFRJ). Doutorando em Direito pela FGV Direito Rio.

Rakel Duque

Mestre em Teorias Jurídicas Contemporâneas pela Universidade Federal do Rio de Janeiro (UFRJ).

Ana Clara Jaccoud

Graduanda da FGV Direito Rio.

Andressa Mota
Graduanda da FGV Direito Rio.

Bruna Crossetti
Graduanda da FGV Direito Rio.

Henrique Korman
Graduando da FGV Direito Rio.

Isabella Marins
Graduanda da FGV Direito Rio.

João Pedro Verbicario
Graduando da FGV Direito Rio.

Pedro Freitas
Graduando da FGV Direito Rio.

Segurança pública na era do big data: Mapeamento e diagnóstico da implementação de novas tecnologias no combate à criminalidade surge a partir do interesse em entender como pesquisas acerca das novas tecnologias podem contribuir para a potencialização da segurança pública na era digital.

Ao adotar uma metodologia exploratória de pesquisa, este trabalho se divide em duas partes: a primeira, dedicada à análise de fontes midiáticas sobre o uso de novas tecnologias pelos órgãos de segurança pública no Brasil, e a segunda composta por entrevistas realizadas com agentes de segurança pública de diferentes órgãos. Com isso, a união entre teoria e prática faz com que a investigação se dê a partir da experiência desses agentes de segurança pública com as novas tecnologias em suas atividades cotidianas, tendo como base, ainda, um estudo quantitativo e qualitativo envolvendo segurança pública e tecnologia em todo o país.