

**UNIVERSIDADE ESTADUAL PAULISTA “JÚLIO DE MESQUITA FILHO”
FACULDADE DE CIÊNCIAS HUMANAS E SOCIAIS**

BÁRBARA GARCIA DE FIGUEIREDO

**IMPLICAÇÕES GEOPOLÍTICAS DO EMPREGO DA
INTELIGÊNCIA ARTIFICIAL EM CENÁRIOS DE
SEGURANÇA**

**Franca
2025**

BÁRBARA GARCIA DE FIGUEIREDO

**IMPLICAÇÕES GEOPOLÍTICAS DO EMPREGO DA
INTELIGÊNCIA ARTIFICIAL EM CENÁRIOS DE SEGURANÇA**

Trabalho de Conclusão de Curso
apresentado à Faculdade de Ciências
Humanas e Sociais da Universidade
Estadual Paulista “Júlio de Mesquita Filho”
como requisito parcial para obtenção do
título de Bacharel em Relações
Internacionais.

Orientadora: Prof^a. Ma. Marianna Braghini
Deus Deu

F475i Figueiredo, Bárbara
Implicações Geopolíticas do Emprego da Inteligência Artificial em Cenários de Segurança / Bárbara Figueiredo. -- Franca, 2025
46 p.

Trabalho de conclusão de curso (Bacharelado - Relações Internacionais) - Universidade Estadual Paulista (UNESP), Faculdade de Ciências Humanas e Sociais, Franca
Orientadora: Marianna Braghini Deus Deu

1. inteligência artificial. 2. segurança pública. 3. geopolítica. 4. Brasil. 5. vigilância eletrônica. I. Título.

BÁRBARA GARCIA DE FIGUEIREDO

**IMPLICAÇÕES GEOPOLÍTICAS DO EMPREGO DA
INTELIGÊNCIA ARTIFICIAL EM CENÁRIOS DE SEGURANÇA**

Trabalho de conclusão de curso apresentado à Faculdade de Ciências Humanas e Sociais da Universidade Estadual Paulista “Júlio de Mesquita Filho” como requisito parcial para obtenção do título de Bacharel em Relações Internacionais.

BANCA EXAMINADORA:

Prof^a. Ma. Marianna Braghini Deus Deu

Prof^a. Dr^a. Mariana da Gama Janot

Prof^a. Dr^a. Marília Carolina Barbosa de
Souza Pimenta

Franca, _____ de _____ de 2025

AGRADECIMENTOS

É fato que, ao longo da graduação, são impostos diversos desafios. Mudar de cidade, conhecer pessoas novas, ter contato com novas realidades e estudar assuntos completamente diferentes do que eu conhecia foram experiências que fizeram parte dessa caminhada. Além disso, também havia dúvidas sobre o futuro e as dificuldades de começar a construir uma vida profissional.

Diante de tudo isso, sinto a necessidade de agradecer às pessoas que foram minha base e tornaram possível essa conquista.

Em primeiro lugar, à minha avó, que foi a principal razão dessa realização. Desde o primeiro dia da primeira escolinha até a entrega deste trabalho, seu apoio e carinho estiveram presentes em todos os momentos. Se não fosse por você, talvez eu não tivesse chegado até aqui.

Ao meu avô, que infelizmente não pôde acompanhar essa etapa, mas que sempre me incentivou a estudar. Tenho certeza de que ele estaria muito orgulhoso.

À minha irmã, Bruna, que acompanhou de perto cada fase da minha vida e foi essencial para que eu conseguisse concluir mais essa etapa.

Agradeço também à UNESP, aos professores e colegas que fizeram parte dessa trajetória e contribuíram de alguma forma para minha formação.

E, em especial, à minha orientadora, Marianna, que ao longo deste último ano me mostrou que a pesquisa pode ser leve, interessante e recompensadora. Sua orientação foi essencial para que este trabalho se tornasse possível.

RESUMO

O trabalho analisa as implicações geopolíticas do emprego da inteligência artificial em cenários de segurança pública, com ênfase no contexto brasileiro e nas transformações provocadas pelo uso dessas tecnologias nas relações entre Estado, sociedade e empresas privadas. Partindo da problemática de que a inteligência artificial não é usada apenas como uma ferramenta objetiva, mas como um instrumento de poder político e econômico, a pesquisa busca compreender de que forma sua aplicação em políticas públicas de segurança acaba aprofundando a dependência tecnológica e a vulnerabilidade geopolítica. O estudo utiliza abordagem qualitativa, fundamentada em revisão bibliográfica e análise documental. A pesquisa tem como objeto de estudo o uso da inteligência artificial aplicada à segurança pública de São Paulo, com foco na atuação do conglomerado de defesa dos Emirados Árabes Unidos, EDGE Group, e sua participação em projetos de segurança como o Muralha Paulista. O trabalho foi estruturado em três partes: a primeira discute os fundamentos teóricos e históricos da inteligência artificial e aborda conceitos como o Capitalismo de Vigilância de Shoshana Zuboff, a interdependência complexa de Joseph Nye e Robert Keohane e o colonialismo de dados de Couldry e Mejias; a segunda apresenta uma análise dos principais sistemas de vigilância em São Paulo, como o Detecta, o City Câmeras, o Smart Sampa e o Muralha Paulista; e, por fim, a terceira examina a atuação do EDGE Group no Brasil e os impactos da sua atuação sobre a soberania digital e a segurança nacional. As conclusões indicam que, embora a inteligência artificial seja apresentada como uma solução para desafios da segurança pública, sua adoção reproduz desigualdades sociais e reforça a dependência brasileira em relação a empresas estrangeiras, configurando um novo tipo de colonialismo tecnológico que desloca o eixo do poder e compromete a soberania dos países do Sul Global.

Palavras-chave: Inteligência artificial; segurança pública; geopolítica; Brasil; vigilância eletrônica;

ABSTRACT

The study analyzes the geopolitical implications of employing artificial intelligence in security contexts, with an emphasis on the Brazilian scenario and the transformations brought about by the use of these technologies in the relations between the State, society, and private companies. Based on the promise that artificial intelligence is not merely a tool but a political and economic instrument of power, the research seeks to understand how its application in public security policies deepens technological dependence and geopolitical vulnerability. The study adopts a qualitative approach, grounded in bibliographic review and documentary analysis. Its object of study is the use of artificial intelligence applied to public security in São Paulo, focusing on the participation of the United Arab Emirates defence conglomerate, EDGE Group, in security projects such as Muralha Paulista. The work is structured into three parts: the first discusses the theoretical and historical foundations of artificial intelligence and addresses concepts such as Shoshana Zuboff's Surveillance Capitalism, Joseph Nye and Robert Keohane's Complex Interdependence, and Couldry and Mejias's Data Colonialism; the second presents an analysis of São Paulo's main surveillance systems, including Detecta, City Câmeras, Smart Sampa and Muralha Paulista;

and finally, the third examines the role of EDGE Group in Brazil and the impacts of its activities on digital sovereignty and national security. The conclusions indicate that, although artificial intelligence is presented as a solution to public security challenges, its adoption reproduces social inequalities and reinforces Brazil's dependence of foreign companies, shaping a new form of technological colonialism that shifts the axis of power and undermines the sovereignty of Global South countries.

Keywords: Artificial intelligence; Public security; Geopolitics; Brazil; Electronic surveillance.

SUMÁRIO

1. Introdução.....	1
2. Capitalismo de vigilância: fundamentos, dinâmica e implicações para a segurança pública e soberania de dados.....	4
2.1 Segurança e legitimação.....	5
2.2 A mercantilização da experiência humana.....	8
2.3 O poder instrumentariano.....	11
3. A inteligência Artificial na Segurança Pública do estado São Paulo.....	14
3.1 Principais sistemas e tecnologias em uso no estado de São Paulo.....	16
3.1.1 Detecta.....	16
3.1.2 City Câmeras de São Paulo.....	17
3.1.3 Smart Sampa.....	18
3.1.4 Muralha Paulista.....	20
4. O conglomerado de defesa – EDGE Group.....	22
4.1 Consolidação do conglomerado de defesa dos Emirados no Brasil e entrada em São Paulo..	24
4.2 O projeto “Bola de Cristal”.....	25
5. Soberania e Geopolítica dos Dados: O Brasil na Era da Vigilância Automatizada.....	27
5.1 Dependência tecnológica e soberania digital.....	28
5.2 O Brasil e a reconfiguração do poder no Sul Global.....	29
6. Considerações Finais.....	31
REFERÊNCIAS.....	32

1. Introdução

Com o fim da Segunda Guerra Mundial em 1945, inicia-se uma nova era de inovações tecnológicas que redefiniriam a sociedade. Entre essas inovações, destaca-se o desenvolvimento de computadores, inicialmente voltados para o aumento da produtividade, o auxílio em tarefas complexas e o processamento de grandes volumes de dados. Tais avanços seriam fundamentais para o surgimento da Terceira Revolução Industrial, marcada pela introdução de robôs, dispositivos digitais e por uma crescente dependência da tecnologia.

Nesse sentido, surge a necessidade de que as máquinas assumam funções antes destinadas apenas aos homens. No entanto, como fazer com que as máquinas “pensem”? Em 1956, acontece o seminário de Dartmouth, em que cientistas, movidos pela ideia de que “todos os aspectos da aprendizagem ou qualquer outra característica da inteligência podem, a princípio, ser descritos tão precisamente que uma máquina pode ser criada para simulá-los.” (McCarthy et al., 1955), buscaram criar máquinas inteligentes que não apenas realizassem cálculos aritméticos, mas também fossem capazes de simular aspectos cognitivos humanos, como o raciocínio, a aprendizagem e mesmo a tomada de decisões.

Esse movimento marca o surgimento da inteligência artificial (IA), campo que, a princípio visto como complementar a matemática, viria a se tornar tão complexo que escaparia tal compreensão e se tornaria uma área completamente independente. Assim, ao longo das décadas seguintes, evoluiria de forma significativa, impulsionada pelo desenvolvimento computacional, pelo aumento no processamento e digitalização de dados e pelo desenvolvimento de algoritmos cada vez mais sofisticados.

Chega-se, então, à chamada Quarta Revolução Industrial. Também conhecida como Indústria 4.0, essa fase é caracterizada pela integração cada vez maior entre sociedade e tecnologia, por meio não só da robótica, mas também pelo rompimento de barreiras através da interconexão de sistemas físicos, digitais e biológicos. Outra característica desse novo mundo é o aumento dos processos de automação e a aceleração no desenvolvimento de inovações. Ainda, a sociedade da indústria 4.0 tem por característica o uso de dados para otimizar a tomada de decisões em ambientes corporativos, sociais, estatais e mesmo

bélicos.

Nesse contexto, os dados passam a exercer um papel de extrema importância, atuando como recurso estratégico não só de Estados, mas também das chamadas *Big Techs* – grandes empresas que dominam o mercado de tecnologia global. A fim de fomentar os códigos e os bancos de suas IAs, esses atores utilizam os mais diversos tipos de informação, como traços de comportamento, localização, preferências de consumo, características físicas e culturais e até mesmo interações sociais. No cenário atual, tudo pode se tornar um dado, contribuindo para a formação do chamado *big data*, que são vastos universos de dados em que uma série de correlações podem ser feitas para se extrair padrões, abrindo caminho para a classificação desses dados.

Segundo Stuart Russell e Peter Norvig (2013), existe um “gargalo do conhecimento” na IA, em que quanto maior o volume de informações utilizado, mais efetivo será o desempenho do algoritmo. Esses algoritmos, por sua vez, podem ser compreendidos como um procedimento computacional bem definido que recebem dados de entrada, executam uma sequência lógica de passos e produzem um resultado como saída, sendo usados para a resolução de problemas específicos e permitindo o processamento de informações e a tomada de decisões (Cormen, 2009). Sendo assim, a “sociedade tecnológica”¹ mostra-se extremamente dependente do fluxo constante de dados, seja para a realização de tarefas simples do cotidiano ou para as mais complexas, como a tomada de decisões políticas, econômicas e de segurança.

Nesse cenário, torna-se possível observar o crescimento da influência das Big Techs, que passam a dominar o cenário global não apenas como prestadoras de serviços, mas também como detentoras de grandes volumes de dados. Com isso, a coleta e o uso das informações contribuem para a sua comercialização, transformando-as em mercadorias extremamente valiosas na sociedade digitalizada contemporânea.

Fica evidente, portanto, que as empresas que controlam os dados, concentram também poder – político, econômico, social e tecnológico. Diante disso, surge uma corrida não só por mercados consumidores de tecnologia, mas também áreas para extrativismo de dados, como por exemplo o Brasil. Por se tratar de um país de dimensões continentais,

¹ O termo “sociedade tecnológica” é usado aqui para descrever o momento histórico em que o avanço das tecnologias passam a influenciar diretamente a forma como as pessoas vivem, produzem e se relacionam. Trata-se de uma sociedade em que a tecnologia digital deixa de ser apenas uma ferramenta e se torna parte da própria estrutura social.

com uma vasta população consumidora de tecnologia, o Brasil apresenta diversas características que o tornam alvo de empresas dos mais variados ramos. Posto isso, embora a inteligência artificial se apresente como uma potencial solução positiva para diversos desafios do país, como o combate ao crime organizado, a violência urbana ou mesmo em questões de vigilância fronteiriça, a ausência de regulamentações específicas sobre o uso e controle de dados levanta preocupações no que tange à soberania digital e à segurança nacional.

O estado de São Paulo, como maior centro urbano, industrial e econômico do Brasil, acaba se tornando um dos principais laboratórios de tecnologia no contexto de segurança pública. A fim de buscar soluções para a prevenção e o combate à criminalidade, cidades como São Paulo, Campinas e São José dos Campos têm investido cada vez mais em sistemas de monitoramento por câmeras inteligentes, tecnologias de reconhecimento facial e até mesmo plataformas de análise de dados. Além disso, São Paulo, por apresentar um volume populacional elevado e infraestrutura tecnológica, desperta o interesse de grandes empresas de tecnologia que buscam testar e expandir soluções digitais por meio da implementação de ferramentas automatizadas. Nesse sentido, o emprego da IA no setor de segurança pública paulista não reflete apenas a busca por soluções no enfrentamento à criminalidade, mas também expõe problemas relacionados à soberania, à concentração de dados por grandes empresas, além de trazer à tona os impactos sociais da vigilância e da segurança cada vez mais robotizadas.

Diante disso, este trabalho propõe investigar as implicações geopolíticas do emprego da inteligência artificial em cenários de segurança, atribuindo ênfase à questão do uso de IAs no setor de segurança pública nas cidades do estado de São Paulo. A pesquisa parte da hipótese de que – embora apresentadas como soluções – essas ferramentas podem ser usadas como perpetuadoras de diversos problemas sociais. Além disso, no que tange ao cenário global, elas também acabam inserindo o Brasil em um contexto de dependência tecnológica – já que grande parte do aparato usado para o monitoramento vem de fora – e também vulnerabilidade geopolítica, frente à concentração global de dados e a atuação das *Big Techs*. Com isso, busca-se compreender os reflexos do uso da IA em políticas de segurança em outras questões, como de soberania e poder no sistema internacional.

Nesse contexto, o trabalho tem como objeto de estudo o uso da inteligência artificial

aplicada à segurança pública no estado de São Paulo, com foco no conglomerado de indústrias de defesa, Edge Group, e a sua atuação em projetos como o Muralha Paulista. A partir disso, busca-se analisar as implicações geopolíticas, sociais e de soberania advindas dessas tecnologias, destacando o papel das empresas privadas no controle de dados.

A pesquisa usará uma abordagem qualitativa, fundamentada na revisão bibliográfica e análise documental. Para isso, o trabalho foi dividido em três partes principais. Inicialmente, é feita uma análise teórico-histórica da Inteligência Artificial e sua evolução no cenário internacional. Nesta seção, são explorados os conceitos como o capitalismo de vigilância de Shoshana Zuboff (2019), que discute a mercantilização da experiência humana e a extração de dados como fonte de poder; na teoria de interdependência complexa de Joseph Nye e Robert Keohane (1977), que ajuda na compreensão da relação entre Estados e empresas transnacionais; e o colonialismo de dados abordado por Couldry e Mejias (2019). Além disso, autores como Didier Bigo e Loïc Wacquant, são utilizados para analisar como as políticas de segurança e as novas tecnologias, embora apresentadas como soluções, acabam reproduzindo desigualdades sociais históricas e justificam práticas de controle.

A segunda parte traça uma linha temporal do desenvolvimento da vigilância por inteligência artificial no estado de São Paulo, analisando os diferentes projetos implementados e suas especificidades técnicas e operacionais. Para embasar essa análise, foram consultadas reportagens jornalísticas, relatórios oficiais e contratos firmados entre governos municipais e estaduais e empresas de tecnologia.

Por fim, a terceira parte faz uma análise da atuação da empresa dos Emirados Árabes, EDGE Group e sua atuação no Brasil, atribuindo foco à sua atuação no estado de São Paulo e no projeto Muralha Paulista. Além de falar sobre sua atuação em outros projetos no Brasil, visando uma expansão da sua atuação no país. Para tanto, foram utilizados releases realizados pela própria empresa, além de publicações dos governos municipais e estaduais.

2.Capitalismo de vigilância: fundamentos, dinâmica e implicações para a segurança pública e soberania de dados

A tecnologia surge como uma ferramenta fundamental para otimizar processos nos mais variados setores – como bélico, político, social ou mesmo corporativo –, além de criar conexões e simplificar o cotidiano geral. A princípio, seu desenvolvimento foi associado à promessa de empoderar indivíduos e democratizar o acesso à informação. Todavia, a crescente dependência tecnológica criou o ambiente perfeito para que as grandes empresas não apenas colem dados através dos seus serviços – amparadas por termos de uso abusivos e cláusulas ambíguas –, mas também monitorem comportamentos, influenciem padrões e, dessa forma, moldem decisões, tudo isso em nome da maximização do lucro e da proteção dos seus próprios interesses. Essa dinâmica constitui as bases do capitalismo de vigilância, conceito desenvolvido pela pesquisadora norte-americana Shoshana Zuboff, que busca descrever um novo estágio do capitalismo contemporâneo, no qual a coleta, o processamento e a comercialização massiva de dados pessoais se tornam o principal motor da acumulação de capital.

Zuboff define também o que chama de “mercados de comportamentos futuros”, que basicamente se pauta na predição dos hábitos de consumo e necessidades das pessoas por meio do chamado *machine learning* (aprendizado de máquina). Dessa forma, ele transforma dados comportamentais – como a voz, personalidade, traços de consumo, emoções – em produtos de previsão que acabam funcionando como mercadoria para empresas e governos, visto que há o interesse em antecipar, manipular ou condicionar o comportamento das pessoas. Por conta disso, a autora afirma que “não basta mais automatizar o fluxo de informação sobre nós; a meta agora é nos automatizar.” (Zuboff, 2021)

2.1 Segurança e legitimação

No contexto de digitalização da vida cotidiana de diferentes nações, Zuboff (2021) mostra como a segurança é usada como artifício para justificar o monitoramento constante e o controle dos dados pelas grandes plataformas. Sob o pretexto de proteção contra ameaças, sejam elas crimes urbanos, terrorismo ou outros problemas cotidianos, as gigantes da tecnologia se consolidam cada vez mais como auxiliares indispensáveis dos Estados, uma vez que fornecem as tecnologias e os algoritmos necessários para que essa vigilância ocorra. Dessa maneira, fica evidente a relação de dependência entre o poder

público e as infraestruturas tecnológicas privadas, ampliando assim os efeitos do chamado capitalismo de vigilância.

Episódios de violência e insegurança podem funcionar como catalisadores para a expansão da vigilância, uma vez que criam cenários em que a sociedade aceita abrir mão da sua liberdade individual em prol de uma suposta segurança coletiva. No Brasil, um exemplo disso ocorreu na cidade do Rio de Janeiro, após a chacina do Jacarezinho, em maio de 2021. Segundo reportagem da Pública (2024), a operação policial resultou na morte de 27 pessoas e foi utilizada como justificativa para a ampliação do uso de sistemas de reconhecimento facial por meio de câmeras públicas em comunidades, além da instalação desses dispositivos nos terminais urbanos de ônibus. A princípio, a Polícia Militar do Estado do Rio de Janeiro (PMERJ) alegou que as políticas de monitoramento tinham como objetivo auxiliar no processo de ocupação e pacificação do território, que tinha grandes registros de violência. No entanto, até 2023, as tecnologias de monitoramento se espalharam também pela região metropolitana do Rio de Janeiro.

Tal lógica se conecta também com o que Didier Bigo (2002) define como “governamentalidade do mal-estar” (*governmentality of unease*). Nesse conceito, inspirado em Michael Foucault (2008), o medo é usado como estratégia para legitimar o fortalecimento dos aparatos de controle social. Logo, o Estado seria responsável por administrar as incertezas da sociedade e, dessa forma, legitimar o fortalecimento dos aparatos de vigilância e controle. Ainda, cabe ressaltar que o controle não se limita à observação, mas também diz respeito à seleção de quem deve ser vigiado, detido ou mesmo deportado, o autor chama esse processo de “banopticon”.

Nesse contexto, Bigo aborda a questão dos imigrantes europeus e como eles são vistos perante a sociedade. A caracterização do imigrante como ameaça ao território, ao povo e à sociedade acaba servindo para justificar políticas de vigilância e restrição. De modo semelhante, Loïc Wacquant (2003) mostra que a pobreza urbana é tratada como problema penal, em vez de questão social. Para Wacquant, o Estado utiliza ferramentas punitivas para lidar com a população pobre, em especial os jovens negros das periferias urbanas. Assim, essa parcela da população acaba sendo vigiada, disciplinada e punida.

No Brasil, essa lógica se aplica à criminalização dos setores marginalizados da população – sobretudo jovens negros e pobres das periferias. Dessa forma, a ampliação do sistema de vigilância após a chacina do Jacarezinho ilustra a operacionalização da

governamentalidade do mal-estar: o medo coletivo acaba sendo usado para justificar a adoção de tecnologias repressivas, responsáveis por aprofundar desigualdades e ampliar o poder punitivo do Estado. O governo, por sua vez, usa de tecnologias digitais para corroborar suas ações, sob o pretexto de torná-las mais precisas e assertivas na neutralização de ameaças.

Logo, a vigilância deixa de ser apenas uma ferramenta e se torna um recurso político-econômico. No contexto de Zuboff, a conexão entre Estado e empresas se dá pela mercantilização de dados e pela legitimação do monitoramento. Assim, o medo da violência urbana em grandes centros, como São Paulo, colabora para que políticas de segurança pública se condicionem cada vez mais à tecnologia vinda de outros países, dando assim, mais poder para um grupo seleto de corporações globais.

Esse condicionamento não se limita apenas ao campo da segurança, mas faz parte de uma complexa estrutura de dependência digital. Segundo estudo desenvolvido pelo Grupo de Estudos em Tecnologias e Inovações na Gestão Pública da Universidade de São Paulo (SILVA et al., 2025), o setor público brasileiro gastou pelo menos R\$ 23 bilhões entre 2014 e 2025 em licenças de software, serviços de computação em nuvem e outras aplicações de empresas estrangeiras – como Microsoft, Oracle, Google e Red Hat. Apenas entre junho de 2024 e junho de 2025, esses gastos somaram R\$10,35 bilhões. Um ponto levantado pelo estudo é que tal quantia seria suficiente para sustentar uma universidade pública como a UnB por quatro anos e meio, fomentando o desenvolvimento tecnológico nacional. Essa política de contratações de empresas estrangeiras evidencia como o Brasil tem adotado um modelo que acaba reforçando sua dependência tecnológica e econômica, em detrimento do fortalecimento da indústria nacional e da pesquisa científica, como também aponta o Jornal da USP (2025).

Os autores do estudo relacionam esse cenário à fragilidade da soberania digital, compreendida como a “capacidade de um Estado exercer controle autônomo sobre seus dados, infraestruturas e decisões sobre tecnologia da informação” (SILVA et al., 2025). A ausência dessa soberania faz com que informações estratégicas fiquem armazenadas em servidores estrangeiros, sob jurisdição de outros países e reféns dos interesses de empresas privadas. Assim, o Brasil se insere em uma situação de “feudalismo digital”, em que as grandes empresas de tecnologia atuam como senhores digitais – manipulando as

ações dos Estados de acordo com as suas vontades e monopolizando o acesso a serviços e políticas públicas. (SILVA et al., 2025)

Dessa maneira, a vigilância automatizada, inicialmente vista como instrumento de segurança, atua como mecanismo de dependência, reforçando a posição periférica brasileira no cenário tecnológico e, principalmente, no cenário de manipulação de dados. O país, ao entregar o controle dos seus dados ao capital estrangeiro, reproduz o que Zuboff (2019) descreve como capitalismo de vigilância: um sistema no qual a informação e o controle são concentrados nas mãos de um seleto grupo de atores que detêm não apenas poder econ, mas também a capacidade de moldar políticas, comportamentos e decisões sociais.

2.2 A mercantilização da experiência humana

Diante de todo o contexto exposto, surge mais uma questão: como as grandes corporações conseguem minerar dados tão sensíveis de forma quase invisível? A resposta está no fato de que, em meio a dispositivos conectados, contas nas mais diversas plataformas, endereços de IP, sensores e câmeras, as *Big Techs* se entranham no cotidiano de modo a transformar qualquer experiência humana em matéria-prima comportamental.

Para Zuboff, essa extração não ocorre apenas de forma consciente ou voluntária, mas também por meio de técnicas preditivas, que capturam informações derivadas de interações, movimentos, relacionamentos, conversas ou até pelas emoções. Tudo isso, ao ser processado pelos algoritmos de *machine learning*, torna-se excedente comportamental, responsável por alimentar modelos de previsão cada vez mais sofisticados, que serão chamados de produtos de predição.

Um exemplo mencionado pela autora é a telemetria, tecnologia que fora desenvolvida por William Mackay para monitorar animais selvagens em ambientes inacessíveis. Essa inovação não tardou em ser utilizada para monitorar seres humanos, uma vez combinada a satélites de alta precisão, sensores e a capacidade preditiva. Dessa forma, tornou-se capaz de revelar comportamentos e deslocamentos de pessoas de forma quase instantânea.

A precisão dos satélites combinada com o crescimento explosivo do poder computacional embutido em minúsculas lascas de silício, sensores avançados, redes adaptadas à internet e analítica preditiva com base em “big data” geraram sistemas extraordinários que revelam os significados e movimentos de populações animais inteiras e seus indivíduos: em qualquer lugar, a qualquer hora. (Zuboff, 2019, p.250-251).

Logo, a mesma infraestrutura usada para rastrear animais selvagens acaba sendo usada para rastrear pessoas. Surge, portanto, o que Zuboff denomina de arquitetura de vigilância difusa, em que “Super-GPS” tornam-se instrumentos de extração e comercialização da experiência humana.

Essa lógica de expropriação é aprofundada também por Couldry e Mejias (2019), que denominam esse fenômeno de “colonialismo de dados” (*data colonialism*). Para os autores, o capitalismo contemporâneo retoma estratégias do colonialismo histórico. No entanto, a *commodity* deixa de ser terras e recursos naturais e passa a ser os dados do cotidiano das pessoas. Dessa forma, novas formas de controle territorial são criadas e fronteiras acabam sendo traçadas por meio da tecnologia.

Posto isso, cidades como São Paulo tornam-se laboratórios dessa mercantilização, sendo usadas tanto para a extração quanto para a venda dos dados. Assim, sistemas de monitoramento de tráfego, câmeras inteligentes e tecnologias de reconhecimento facial desempenham papel fundamental na infraestrutura de vigilância preditiva. O espaço urbano, em toda sua complexidade de interações, torna-se um campo informacional, no qual a ação do indivíduo serve de combustível para o desenvolvimento de estratégias de segurança, marketing ou controle social.

Um exemplo dessa dinâmica de mercantilização humana e colonialismo de dados é o caso da Clearview AI, empresa norte-americana especializada em reconhecimento facial. Segundo uma matéria publicada pelo jornal The Intercept Brasil (2025), a empresa de inteligência artificial detém hoje um banco de dados com mais de 20 bilhões de imagens de pessoas do mundo todo, sendo que cerca de 3 bilhões são da população brasileira. Ainda, esses dados são coletados por meio da raspagem de conteúdos disponíveis na internet, como redes sociais, sites de notícias, imagens de eventos e do espaço urbano.

O funcionamento do software da Clearview se dá ao vasculhar a internet a fim de identificar, copiar e armazenar rostos, criando assim um banco de dados sem qualquer consentimento dos indivíduos. Essa base, então, é oferecida a governos, instituições policiais e agências de segurança pública como solução para a identificação de suspeitos e monitoramentos das cidades.

Segundo The Intercept (2023), no Brasil, o Ministério da Justiça e a Polícia Civil de São Paulo já fazem uso da tecnologia. Em setembro de 2022, o Ministério da Justiça e Segurança Pública realizou a contratação da Clearview dentro do Projeto Excel, programa destinado à investigação criminal, visando o combate a organizações criminosas. No entanto, o contrato foi mantido em sigilo até 2025, o que expõe uma fragilidade regulatória frente a coleta e uso dos dados biométricos de brasileiros.

Além disso, em dezembro de 2024, o Senado Federal adquiriu uma licença do software para a Polícia Legislativa para a aplicação em investigações internas. Enquanto isso, em países europeus, o uso do sistema foi proibido ou restringido, justamente por violar normas de proteção de dados, como os apresentados no Regulamento Geral de Proteção de Dados (GDPR). No Brasil, todavia, lacunas na aplicação da Lei Geral de Proteção de Dados (LGPD) permitem que tecnologias como as produzidas pela Clearview se tornem ferramentas dos governos, consolidando a dependência do Estado em relação às agências de tecnologia estrangeiras, aprofundando a lógica do capitalismo de vigilância e do colonialismo de dados.

Outro caso recente que evidencia a mercantilização da experiência humana é o da Tools for Humanity, responsável pelo projeto World ID, cujo fundador é Sam Altman, também CEO da Open AI, que abriga o ChatGPT. De acordo com dados da Tools for Humanity, o World ID é um projeto que busca criar uma verificação universal das pessoas por meio da íris humana. A partir do seu registro, a íris funcionaria como uma digital e seria usada para verificar que o indivíduo é humano, permitindo então acesso a sites, bancos, transações, etc. Para tanto, a empresa oferecia algum tipo de recompensa a fim de comprar os dados biométricos do usuário – como Worldcoin (WLD), token digital que poderia valer de R\$300 a R\$700. No entanto, a prática de coleta de dados biométricos pela empresa foi barrada pela Autoridade Nacional de Proteção de Dados (ANPD).

Segundo a ANPD, ao condicionar o consentimento dos participantes a algum tipo de bonificação econômica, haveria um comprometimento da liberdade de decisão, colocando os usuários em uma situação de vulnerabilidade e indo contra os princípios da Lei Geral de Proteção de Dados (LGPD). Mesmo após a suspensão em janeiro de 2025, a empresa tentou recorrer da decisão por meio da reformulação do projeto, que passaria a funcionar através de um sistema de indicações, no qual os usuários receberiam benefícios ao indicar

novas pessoas a participarem do escaneamento. A autoridade, no entanto, reconheceu que ainda assim haveria uma bonificação, ainda que indireta, e manteve a proibição.

O episódio deixa claro como práticas de extração de dados biométricos são vendidos como inovação tecnológica e inclusão digital, mas na realidade operam dentro da mesma lógica de expropriação descrita por Zuboff (2019) e Couldry e Mejias (2019). A experiência humana – ou mesmo o próprio corpo, convertido em dados biométricos – é transformada em ativo econômico. Assim, a coleta da íris deixa de ser uma etapa de autenticação e passa a integrar o esquema global de exploração de dados, em que identidades são tratadas como *commodities*.

2.3 O poder instrumentariano

O conceito de poder instrumentariano, formulado por Zuboff (2019), descreve uma nova lógica de controle social e econômico operada pelas empresas de tecnologia no contexto do capitalismo de vigilância. Diferente de outras formas de dominação baseadas na coerção física ou no autoritarismo, o poder instrumentariano atua por meio da coleta massiva de dados e da modulação do comportamento por meio de sistemas algorítmicos e da inteligência artificial.

Para contextualizar essa nova organização de poder, a autora introduz o conceito de “Grande Outro” (*Big Other*), uma estrutura onipresente, composta por um grande aparato tecnológico responsável por influenciar o comportamento humano. Ao contrário do “Grande Irmão” orwelliano, em que o controle é visível, autoritário e busca a repressão, o Grande Outro é caracterizado por uma vigilância automatizada, que se insere na sociedade de forma silenciosa. Ele não visa a repressão direta, mas a extração de características dos indivíduos, que serão transformados em insumos para o *machine learning*.

No cenário internacional, esse novo arranjo de poder se conecta à teoria da interdependência complexa, proposta por Robert Keohane e Joseph Nye (1977), segundo a qual os Estados compartilham o poder com atores não estatais, como corporações tecnológicas transnacionais. Nesse contexto, as gigantes da tecnologia – como Apple, Amazon, Google e Meta – ganham espaço e tornam-se agentes centrais ao exercerem suas ações e influenciarem o comportamento humano por meio de algoritmos e plataformas digitais. Assim, conseguem moldar preferências e decisões de acordo com

seus interesses econômicos e estratégicos. Dessa forma, essas empresas passam a interferir diretamente sobre o sistema internacional, controlando tecnologias indispensáveis, impactando políticas públicas e acumulando recursos que superam o PIB de muitos países, como evidenciado pela matéria da BBC News Brasil (2020). Fica evidente, portanto, o compartilhamento de poder, que antes era exclusivo dos Estados.

Essa ação pode ser observada em casos como o Projeto de Lei das Fake News (PL 2630/2020), em que empresas como o Google e a Meta lideraram campanhas contra a proposta que atribuiria regulamentações para as redes sociais. Segundo a matéria do The Intercept (2023), essas empresas foram responsáveis por mobilizar campanhas publicitárias, manipular mecanismos de busca e pressionar parlamentares, contribuindo assim para que o projeto fosse deixado de lado pela Câmara. O episódio deixa claro como decisões públicas são condicionadas pelos interesses das corporações, deslocando o eixo da soberania estatal para as *Big Techs*.

Outro ponto importante no que tange ao pensamento de Zuboff diz respeito à crença de que o poder instrumentariano seria uma forma de poder não violenta. No entanto, ainda que tal método de controle esteja presente no cotidiano das pessoas de forma discreta, sendo caracterizado pela autora como uma forma de dominação não violenta – visto que não depende da coerção física nem da violência explícita, mas sim da modulação comportamental –, sua aplicação prática mostra padrões de seletividade e desigualdade. Softwares de monitoramento e reconhecimento facial, muitas vezes programados por meio de algoritmos enviesados, acabam tendo como alvo grupos sociais vulneráveis, como imigrantes, negros e moradores da periferia. Essa seletividade deixa evidente que a tecnologia, embora disfarçada de neutralidade, acaba atuando como instrumento de repressão.

Essa ideia de que o poder instrumentariano seria uma forma de controle “não violenta” é também problematizada por Peron e Röhe (2024), que introduzem o conceito de silenciamento sociotécnico visando evidenciar como a aparente neutralidade das tecnologias esconde suas dimensões políticas e discriminatórias. Segundo os autores, ao operar por meio de algoritmos opacos e processos automatizados, os algoritmos produzem um efeito de invisibilidade sobre as formas de dominação, tornando a violência imperceptível. Trata-se de um processo de apagamento mascarado dos conflitos e das decisões humanas que moldam esses sistemas.

Nesse sentido, a suavidade descrita por Zuboff não representa a ausência de violência, mas sim uma forma de violência silenciada. Essa violência deixa de ser explícita e passa a se manifestar por meio de algoritmos, da predição dos riscos e da modulação dos comportamentos, reproduzindo desigualdades sob discurso de eficiência tecnológica. Esse silenciamento sociotécnico reforça, portanto, como o poder instrumentariano atua de forma seletiva, disfarçando a dominação sobre determinados grupos sociais por meio da aparência de neutralidade.

Uma das formas em que isso se torna claro é na criminalização da miséria, conceito desenvolvido por Loïc Wacquant. O autor analisa o caso dos Estados Unidos, visando mostrar como a lógica de um Estado de providência – que, ainda que de forma limitada, buscava amenizar a miséria da população – foi substituída por um Estado penal. Para tanto, Wacquant mostra que as políticas sociais que garantiam alguma estabilidade para grupos marginalizados foram desmontadas e terceirizadas, enquanto seus recursos foram destinados para o estabelecimento de medidas repressivas e para o fortalecimento do aparato policial e carcerário. Trata-se, segundo o autor, de um Estado híbrido: ele não possui as características de um “Estado mínimo” e não-intervencionista, pois mantém certos programas assistenciais. Todavia, esses programas são cada vez mais restringidos a grupos específicos e privilegiados. Além disso, o Estado utiliza tais mecanismos de exclusão como forma de disciplinar segmentos da população considerados inferiores ou perigosos.

Essa substituição da guerra contra a pobreza pela guerra contra os pobres deixa explícita a seletividade das políticas estatais. Wacquant mostra como os Estados Unidos passaram a dificultar e a burocratizar o acesso à assistência social, enquanto os investimentos no sistema penal se multiplicavam. De acordo com a sua análise, o encarceramento – que cresceu mais de 300% entre 1970 e 1990 e cuja população é majoritariamente composta por negros e latinos – exemplifica o papel da punição como forma de gestão da desigualdade. Já os serviços sociais passam a se tornar instrumentos de vigilância e de controle, condicionando o acesso a benefícios ao cumprimento de normas de conduta moral, familiar e burocrática.

Essa lógica descrita por Wacquant ajuda a compreender a aplicação prática do poder instrumentariano no Brasil. Ainda que Zuboff defenda que o controle algorítmico seja uma forma não violenta de poder, sua implementação concreta demonstra um grau de

seletividade e desigualdade quando aplicados na sociedade. Sistemas de reconhecimento facial, por exemplo, reproduzem os mesmos padrões de criminalização das populações marginalizadas, atuando como uma ferramenta tecnológica da repressão policial. No contexto brasileiro, essa dinâmica se evidencia no dado de que 90,5% das prisões realizadas por reconhecimento facial no país tinham como alvo pessoas negras (Rede de Observatórios de Segurança, 2019). Logo, a tecnologia, apresentada como neutra e objetiva, é usada como instrumento de vigilância e repressão seletiva, reforçando desigualdades sociais.

3. A inteligência Artificial na Segurança Pública do estado São Paulo

A Quarta Revolução Industrial é marcada pelo avanço de tecnologias cada vez mais sofisticadas, capazes de processar grandes volumes de dados em um curto espaço de tempo. Esse movimento torna-se bastante claro ao se comparar um computador dos anos 2000 com um dispositivo mais recente: mais veloz, integrado e, sobretudo, mais vinculado ao cotidiano das pessoas. Nesse cenário, empresas de tecnologias desenvolvem ferramentas não apenas para atender as necessidades dos consumidores e do capital privado, mas também para governos, ampliando assim sua influência sobre o mercado e sobre as políticas públicas.

Nesse contexto, a IA se apresenta como uma solução multifuncional, aplicada desde atividades administrativas – Como o uso de IA pelo Departamento de Água e Esgoto de Jundiaí para detecção de vazamentos – até funções ligadas diretamente ao controle social, como sistemas de análise preditiva de criminalidade, monitoramento e reconhecimento facial.

Essa tendência acaba não sendo limitada apenas ao Brasil. Como destaca Souza (2018), nas últimas décadas, houve um aumento global na incorporação de tecnologias digitais de segurança pública, impulsionado por um discurso de eficiência e modernização. Tal discurso é frequentemente sustentado pela promessa de que essas tecnologias podem auxiliar na redução da criminalidade, aumentar a eficácia policial e otimizar recursos. No entanto, a implementação dessas tecnologias, especialmente no Sul Global, é realizada por meio de parcerias com grandes empresas de tecnologia estrangeiras, que controlam o

acesso às ferramentas e os dados gerados por essas ferramentas, gerando assim dependência tecnológica e riscos à soberania.

No Brasil, o crescimento da dependência tecnológica cresce cada vez mais. Segundo dados da revista *Veja* (2024), o setor de tecnologia apresentou um crescimento de 86,2% entre janeiro de 2020 e junho de 2024, representando cerca de 3,2% do Produto Interno Bruto (PIB) do país. No entanto, grande parte da tecnologia do Brasil vem de fora, o que pode representar grande risco à soberania digital. De acordo com uma análise realizada pela empresa *Efficienza Negócios Internacionais* (2025), as importações de produtos tecnológicos – como servidores de alto desempenho, sensores inteligentes, drones, robôs, entre outros equipamentos de informática e telecomunicações –, tiveram um aumento de 15% somente no primeiro semestre de 2025, representando cerca de US\$ 9,8 bilhões. Fabio Coelho, presidente do Google no Brasil, já alertou que, sem investimentos nacionais no setor da IA, o Brasil permanecerá refém das tecnologias estrangeiras, o que pode prejudicar setores estratégicos, como a segurança pública e o controle sobre os dados da população.

O estado de São Paulo, maior polo econômico e urbano do Brasil, ocupa posição estratégica nesse cenário. Com uma economia diversificada, voltada tanto para o setor industrial quanto para o agronegócio, e uma avançada infraestrutura tecnológica, o estado reúne características que o fazem atuar como um laboratório de experimentação de sistemas de vigilância. Sua densa rede de transportes, elevada densidade populacional e grande fluxo de dados criam o ambiente ideal para que empresas privadas testarem e expandam soluções de segurança baseadas em inteligência artificial.

Além disso, a elevada taxa de urbanização traz consigo desafios relacionados à gestão de grandes centros, como as significativas taxas de criminalidade ou mesmo problemas relacionados à administração. Tudo isso, faz com que a busca por soluções tecnológicas sejam incentivadas.

Nesse contexto, observa-se a convergência de interesses entre o poder público e as corporações privadas, processo que reflete a lógica descrita por Zuboff (2019) sobre o capitalismo de vigilância, na qual empresas detentoras de tecnologia e dados passam a condicionar decisões governamentais. Nessa dinâmica, o fornecimento de soluções tecnológicas cria uma dependência que extrapola o campo operacional e passa a impactar diretamente a soberania digital e a autonomia das políticas de segurança. Com o setor de

segurança cada vez mais concentrado nas mãos de atores estrangeiros, abre-se espaço para que interesses corporativos moldem prioridades nacionais e locais, descolando parte do poder do Estado para essas corporações.

É nesse cenário que se insere o conceito desenvolvido por Peron e Alvarez (2021) de “sociabilidade securitária”, em que cidadãos, empresas e Estados dividem o controle e a responsabilidade pela vigilância. Para os autores, esse modelo emerge de um processo histórico de descentralização da segurança, iniciado nas décadas 1970, com práticas de policiamento comunitário e vigilância de vizinhança. Em São Paulo, essa tendência fica evidente por meio da interação entre o setor público e empresas de tecnologia. É nesse contexto que se insere a atuação de grandes corporações de tecnologia, como o conglomerado de defesa EDGE Group, que vêm direcionando investimentos e realizando parcerias estratégicas visando fornecer tecnologias de vigilância e segurança pública.

3.1 Principais sistemas e tecnologias em uso no estado de São Paulo

Em função da sua relevância econômica e seus diversos desafios urbanos, o estado de São Paulo se consolidou como polo de implementação de tecnologias de segurança pública. Nesse contexto, surgem iniciativas que vão desde o uso de câmeras inteligentes e reconhecimento facial em áreas de grande circulação, até plataformas de análise preditiva capazes de antecipar padrões criminais. A implementação dessas ferramentas envolve não apenas o governo do estado, mas também empresas nacionais e internacionais, conectando a esfera local a redes globais de fornecimento tecnológico.

Diante desse quadro, surgem diversos projetos relacionados a Sistemas Inteligentes, como: o Sistema de Informações Criminais (INFOCRIM), a Base Informatizada de Fotografias Criminais (FOTOCRIM), o Sistema de Informações Operacionais da Polícia Militar (SIOPM) e o Centro de Operações da Polícia Militar (COPM). Além disso, há também investimentos em tecnologias de videomonitoramento e integração de dados. A seguir, será desenvolvida uma análise sobre os principais projetos de vigilância automatizada que vêm sendo implementados no estado de São Paulo.

3.1.1 Detecta

O Detecta foi lançado em 2014 pela Segurança Pública de São Paulo e busca usar inteligência artificial e análise de dados para criar um banco de dados integrado às polícias Militar, Civil e Científica. O projeto tem como objetivo acompanhar, em tempo real, ocorrências no estado para auxiliar no combate ao crime.

O sistema é alimentado por meio de ferramentas específicas, como Leitores Automáticos de Placas (OCR), câmeras de videomonitoramento – públicas ou privadas –, softwares de vídeo analítico e sensores. Além disso, conta com a integração de câmeras acopladas a veículos e equipamentos da polícia, ampliando a coleta e o cruzamento de dados. Dessa forma, o projeto promete uma maior agilidade na identificação de ocorrências e na tomada de decisões dos agentes de segurança pública.

Em 2015, o Detecta buscou implementar o chamado Cinturão Eletrônico. Segundo dados da Secretaria de Segurança Pública, o projeto integrou 2661 câmeras, sendo 480 câmeras OCR, responsáveis pela leitura de placas de automóveis, e 2181 câmeras de videomonitoramento comum, distribuídas em 38 cidades da faixa litorânea, entre o Vale do Ribeira e o Vale do Paraíba. O objetivo dessa fase era monitorar o fluxo de veículos que cruzavam a região, avisando tanto sobre situações adversas do trânsito, como veículos no acostamento, como também infrações ou veículos roubados.

O funcionamento do Detecta se dá por meio de um convênio firmado entre o governo do estado de São Paulo, os municípios e as empresas que atendam aos requisitos impostos. Entre as necessidades estabelecidas estão o repasse de dados de interesse para a Segurança Pública, a garantia de sigilo e segurança dos dados coletados e o compartilhamento de imagens, radares e dados de videomonitoramento. Assim, a eficácia do projeto está ligada à cooperação entre estado, municípios e o setor privado, criando uma relação de interdependência.

3.1.2 City Câmeras de São Paulo

Enquanto o Detecta marcou uma nova tentativa do estado de São Paulo de implementar projetos de vigilância, o City Câmeras, lançado em 2017 pela Prefeitura de São Paulo, teve como objetivo expandir o monitoramento urbano e reduzir custos por meio da integração entre câmeras públicas, privadas e residenciais. Desenvolvido como política

de segurança pública, seria usado como base para o programa Smart Sampa, considerado pela prefeitura o maior sistema de monitoramento da América Latina.

O diferencial dessa iniciativa foi a tentativa de envolver cidadãos e o setor privado na construção de uma rede de vigilância, descentralizando o controle estatal e promovendo o discurso de uma segurança colaborativa. Segundo matéria da Veja São Paulo (PAULO, 2023), durante a implementação do programa, diversas empresas do setor de vigilância e segurança privada buscaram firmar contratos com a prefeitura de São Paulo, visando comercializar seus produtos e serviços. Nesse sentido, fica evidente a interdependência entre políticas públicas e interesses corporativos no campo da segurança.

Apesar da proposta tida como inovadora, encontrou baixa adesão devido às barreiras econômicas e à falta de garantias quanto à proteção dos dados compartilhados. A necessidade de aquisição de câmeras de alta resolução com acesso à internet, os custos de manutenção e o pagamento pelo armazenamento em nuvem tornaram o programa pouco acessível. Segundo a Veja (QUINTELLA, 2021), a exigência de que a população arcasse com os custos do armazenamento foi um dos principais motivos para a baixa participação. Assim, o City Câmeras revela como políticas de vigilância urbana no Brasil se estruturam a partir de parcerias público-privadas, transferindo custos e responsabilidades à população sob discurso de cooperação pela segurança.

3.1.3 Smart Sampa

A fim de dar continuidade ao projeto de vigilância em São Paulo, a prefeitura iniciou, em 2024, o projeto Smart Sampa. Desenvolvido pela Secretaria Municipal de Segurança Urbana (SMSU), o programa visa integrar as imagens obtidas a partir de câmeras públicas e privadas em um único banco de dados, criando assim uma rede de monitoramento.

De acordo com a Prefeitura de São Paulo, em 2023 foram instaladas aproximadamente 20 mil câmeras com tecnologia de reconhecimento facial, integradas aos sistemas municipais de monitoramento. Conforme noticiado pelo Mobile Time (MEDEIROS, 2023), a instalação tinha como objetivo ocorrer em locais estratégicos da cidade de São Paulo, como escolas, parques, unidades de saúde e outras áreas de grande circulação. A distribuição das câmeras seguiu critérios geográficos no que diz respeito a sua distribuição: cerca de 6 mil na zona leste, 4,5 mil na zona sul, 3,5 mil na zona oeste, 3,3 mil na região

central e 2,7 mil na zona norte. Segundo o secretário Adjunto de Segurança Urbana, Junio Fagotti, o objetivo do projeto é gerar um efeito preventivo, aumentando a agilidade na tomada de decisões dos mecanismos de segurança.

A Monuv, responsável pelo processamento em nuvem dos dados captados, atua como parceira da Prefeitura no que tange ao processamento e armazenamento das informações coletadas. O sistema do projeto integra dados obtidos de órgãos públicos como CET, SPtrans, CPTM, Metrô, SAMU, Polícias Civil e Militar. Além disso, utiliza a leitura de placas de veículos por meio de câmeras LRV, além da utilização de reconhecimento facial. Segundo informes da própria plataforma, essa integração possibilitou a prisão de procurados pela justiça, prisões em flagrante, localização de pessoas desaparecidas e redução de roubos e furtos ao longo de 2023 e 2024.

Todavia, seu software é programado para filtrar indivíduos por meio de suas características, como cor, face e características físicas. Segundo matéria do UOL (AUGUSTO, 2022), o edital do projeto previa considerar situações de “vadiagem” e “tempo de permanência” como atitudes suspeitas. Ainda, segundo o pesquisador Luan Cruz ao UOL (AUGUSTO, 2022), as câmeras não são capazes de ser 100% assertivas no reconhecimento, podendo reconhecer erroneamente uma pessoa, sendo pessoas negras as mais acometidas pelos erros.

Outro ponto importante sobre o projeto diz respeito a sua efetividade. De acordo com os dados divulgados pela prefeitura por meio do “Prisômetro” – painel do Smart Sampa instalado no centro da cidade com os números de foragidos, presos e pessoas encontradas pelo projeto –,

“Desde o início da operação do Smart Sampa, em que as câmeras com tecnologia de reconhecimento facial e algoritmos avançados que identificam e localizam pessoas cadastradas em vários sistemas, foram presos em flagrante 1.902 criminosos, 720 condenados foragidos da Justiça e localizadas 41 pessoas que estavam desaparecidas” (Prefeitura de São Paulo, 2025)

Entretanto, devido a falta de efetividade e garantias, diversos erros são cometidos. De acordo com o Metrôpoles (Henrique, 2025), o projeto chegou a indicar um Cabo da PM como foragido por homicídio. Já o UOL (Araújo; Vespa, 2025) relatou o caso de um idoso que foi confundido com um estuproador enquanto prestava serviço voluntário em uma UBS de São Paulo. Segundo o professor de direito da USP, Guilherme Madeira Dezem, ao UOL (ARAÚJO; VESPA, 2025), “enquanto se divulga um placar de pessoas presas,

escondem-se os erros do sistema – e, principalmente, quem são os alvos desses erros. ‘Em geral, são pessoas negras e periféricas’”.

Essas críticas são reforçadas pelo estudo “O Panóptico: Smart Sampa vigia, mas não protege” (CESeC, 2025), que evidencia a falta de comprovação da redução da criminalidade pelo projeto na cidade de São Paulo. Segundo o relatório, o Smart Sampa promove uma falsa eficiência, baseada na produtividade policial – por meio de prisões e abordagens –, no entanto, ignora o impacto do projeto na segurança pública. Ainda, o CESeC destaca como a vigilância tem servido como instrumento de controle social, perpetuando desigualdades raciais e territoriais, reforçando a seletividade das medidas de punição.

Nesse sentido, críticos como Alcides Peron (2024) apontam que esses sistemas integrados de vigilância colocam em risco não apenas a privacidade dos indivíduos, mas também direitos fundamentais. Para o autor, o avanço dessas tecnologias insere a segurança pública nas mãos de empresas privadas, que passam a definir quem deve ser monitorado e sob quais critérios.

Dessa forma, o Smart Sampa não representa apenas uma modernização das ferramentas de monitoramento da polícia paulista, mas sobretudo a consolidação de um modelo de vigilância automatizada que privilegia indicadores e métricas em detrimento da proteção efetiva das pessoas, reproduzindo práticas de desigualdade estrutural sob discurso de inovação tecnológica.

3.1.4 Muralha Paulista

Instituído pelo Governo do Estado de São Paulo em setembro de 2024, o Muralha Paulista busca aprofundar as políticas de monitoramento iniciadas com o Detecta, ampliando massivamente seu alcance ao envolver os municípios paulistas. O programa de vigilância integrada tem como objetivo controlar a mobilidade criminal no território paulista, ampliando a probabilidade de prisões, além de estruturar políticas de segurança pública baseadas em tecnologia (UNIFESP, 2024).

O projeto parte da premissa de que a criminalidade pode ser controlada por meio de intervenção de ferramentas de monitoramento, utilizando soluções tecnológicas como câmeras de vigilância, sistemas de leitura automáticas de placas e cruzamento de

informações com banco de dados governamentais, como os do Detran, da Polícia Civil ou da Polícia Militar (SSPSP, 2024). Nesse sentido, o programa não apenas monitora, mas opera dentro de uma lógica preditiva, em que padrões criminais são inferidos e comportamentos podem ser antecipados.

Essa perspectiva dialoga com as discussões apresentadas por Zanabria et al. (2020) no estudo *CrimAnalyzer: Understanding Crime Patterns in São Paulo City*. Os autores mostram como o uso de grandes volumes de dados pode mapear e prever pontos de concentração de crimes na cidade de São Paulo, a partir de padrões espaciais e temporais. Embora o foco do artigo seja uma análise técnica, voltada para a eficiência da gestão da segurança pública, ele compactua da mesma lógica que sustenta o Muralha Paulista: a de que o crime pode ser compreendido por meio do cruzamento de informações e do *machine learning*. A pesquisa evidencia que determinados tipos de crime seguem padrões previsíveis, relacionados a fatores como horário, localização e estrutura urbana. Na prática, reforça a ideia de que a violência pode ser administrada a partir de dados, reduzindo a complexidade do problema a uma questão de gestão tecnológica.

Por outro lado, o boletim “Uma muralha invisível: controles a céu aberto, monitoramentos e a polícia preditiva” (LASinTec/UNIFESP, 2024) faz um contraponto com essa visão. O texto destaca como o Muralha Paulista não apenas utiliza da tecnologia, mas cria também novas formas de poder, ao articular o controle estatal e a atuação de empresas privadas sob o discurso da segurança pública. Em vez de apenas reagir ao crime, o policiamento preditivo antecipa e cria cenários de risco, exercendo controle constante da população. Nesse contexto, a suposta neutralidade dos algoritmos funciona como uma maneira de gerir a população e o território, reforçando desigualdades sociais que já existem.

Apesar da promessa de identificar suspeitos, localizar pessoas desaparecidas e rastrear veículos – apresentada à população como inovação tecnológica –, na prática o sistema funciona como um modelo de policiamento preditivo. Assim, dados do dia a dia são coletados e utilizados pelos agentes de segurança para agilizar a tomada de decisões. O problema é que, a fim de programar os dispositivos e softwares, aplica-se uma filtragem algorítmica que acaba marginalizando grupos específicos (UNIFESP, 2024).

Segundo Alcides Peron, em entrevista à Agência Brasil (MELLO 2024), o Muralha é capaz de processar um elevado número de informações, levando precisamente a

indivíduos. A plataforma é conectada a sistemas do Governo Federal que permitem o acesso a informações que vão desde mandados de prisão a números de Cadastro de Pessoa Física (CPF).

Ainda que o governo aponte uma adesão de mais de 500 municípios do estado de São Paulo ao programa até 2025 e prometa investimentos expressivos no setor de vigilância, há críticas quanto à priorização desse modelo de segurança. Como apontado pela UNIFESP (2024), o aumento de políticas de vigilância amplia o poder de coerção do Estado, e acaba falhando em reduzir as causas dos reais problemas estruturais da violência, além de retomar lógicas de marginalização historicamente conhecidas. Assim, mais do que representar inovação tecnológica, o Muralha Paulista reforça práticas punitivas e de controle social que sustentam desigualdades já existentes.

Dessa forma, o Muralha Paulista não representa apenas a modernização das políticas de segurança pública no estado de São Paulo, mas também revela um movimento de dependência tecnológica e securitária. A expansão dos sistemas baseados em inteligência artificial e vigilância automatizada acaba inserindo o Brasil em uma lógica de defesa em que a tecnologia passa a ocupar um papel central na gestão da segurança. Nesse contexto, empresas internacionais como o EDGE Group ganham destaque ao fornecer soluções que vão desde o monitoramento urbano até aplicações militares, consolidando um mercado de defesa que ultrapassa as fronteiras estatais e ressalta os desafios da dependência tecnológica, da soberania nacional.

4. O conglomerado de defesa – EDGE Group

Fundado em 2019, o conglomerado de tecnologia árabe, EDGE Group vem se consolidando no setor de defesa e tecnologias de vigilância, com aparatos que vão desde sistemas autônomos e mísseis até soluções de monitoramento e guerra eletrônica. Desde sua criação, o grupo adota uma estratégia de internacionalização marcada pela aquisição de empresas locais e pelo fechamento de parcerias estratégicas, ofertando tecnologias voltadas tanto para fins militares quanto para segurança pública.

No Brasil, sua presença data de maio de 2022, quando uma delegação militar brasileira realiza uma visita à sede do grupo nos Emirados Árabes Unidos para discutir possíveis parcerias. A partir daí, dá-se início a uma acelerada aproximação que, em pouco

mais de dois anos, resultaria em acordos bilionários, aquisições de empresas e a instalação de um escritório do grupo voltado para a sua expansão na América Latina. Segundo a CNN Brasil, o conglomerado já teria investido mais de R\$3 bilhões no país (GARCIA, 2024).

De acordo com publicações do EDGE em suas mídias sociais (EDGE, 2023), a participação do grupo na LAAD Defense & Security – a maior feira de defesa e segurança da América Latina, restrita a forças policiais, forças armadas, autoridades e profissionais dos setores de segurança e defesa – em 2023, foi responsável por consolidar a atuação do EDGE no Brasil. Durante o evento, o conglomerado fechou diversos acordos, dentre eles com a Marinha do Brasil, visando o desenvolvimento de mísseis antinavio de longo alcance, e também com empresas como Condor, SIATT e Akaer. Ainda nesse ano, em setembro, formaliza a compra de 50% da SIATT, integrando-se ao projeto MANSUP-ER, focado no desenvolvimento de um míssil antinavio com alcance de 200km (GARCIA, 2025), além de assinar diversas parcerias com os setores das Forças Armadas Brasileiras. Todavia, sua atuação não se restringe apenas ao setor militar, nos últimos anos a empresa vem investindo e ampliando sua atuação no segmento de segurança pública, fechando diversas parcerias com governos estaduais, como o Governo no Estado de São Paulo, para o fornecimento de tecnologias de vigilância, análise preditiva e integração de dados.

Assim, no estado de São Paulo, sua atuação começa a ser efetivada a partir de agosto de 2023, com uma visita de representantes do governo à empresa, a fim de discutir acordos de cooperação. Em 2024, é anunciado o projeto “Bola de Cristal” (*Crystal Ball*), que, de acordo com matéria do Metrôpoles (RIBEIRO; RESK, 2024), caracteriza-se como uma iniciativa de segurança pública que combina câmeras inteligentes, sistemas de comando e controle, drones, análise preditiva e IA para monitorar determinadas regiões da cidade de São Paulo. Pouco tempo depois, o acordo acaba sendo ampliado e São Paulo passa a ser usada como cidade modelo para outros centros da América-Latina aderirem às tecnologias disponibilizadas pelo EDGE.

Todo esse contexto torna evidente a velocidade com que o grupo se estabeleceu no país. Além disso, deixa claro como o Brasil e, principalmente, o estado de São Paulo acabam sendo usados como laboratório para a testagem de novas tecnologias, além de se tornarem peças fundamentais para a consolidação e expansão da empresa na América Latina. Assim, o grupo EDGE, ao vincular sua atuação nos setores comerciais, militares e

de segurança pública, reforça sua posição como ator chave na interseção entre defesa, segurança e governança, abrindo espaço para uma análise sobre as implicações geopolíticas e sociais das suas ações.

4.1 Consolidação do conglomerado de defesa dos Emirados no Brasil e entrada em São Paulo

Como mencionado anteriormente, o EDGE Group vem se estabelecendo rapidamente no país, firmando parcerias em setores estratégicos da defesa e tecnologia. Para além dos acordos bilionários com a Marinha do Brasil e da aquisição de empresas como a SIATT e a Condor, o conglomerado árabe vem assinando memorandos de entendimento – acordo em que duas ou mais partes expressam suas intenções, termos e condições para uma eventual cooperação – com empresas nacionais, como a AKAER, voltada para engenharia aeroespacial, e a Turbomachine, especializada na produção de turbinas a gás. Em paralelo com os acordos voltados para as empresas, o grupo tem buscado cooperação também em nível regional. Como exemplo disso, tem-se o acordo firmado em 2023 com o Governo do Estado do Rio de Janeiro e a parceria com o Corpo de Fuzileiros Navais. De acordo com publicações realizadas pelos canais oficiais da Marinha brasileira nesse mesmo ano, a parceria era voltada para o desenvolvimento de veículos autônomos e sistemas de guerra eletrônica.

Outro ponto importante na trajetória do EDGE Group no Brasil ocorreu na cidade de São José dos Campos – importante polo na área de inovação tecnológica e aeroespacial do país, abrigando instituições como Akaer, SIATT e o Instituto Tecnológico de Aeronáutica (ITA) – onde a empresa celebrou acordos visando tanto a expansão quanto a formação de mão de obra qualificada (Agência Nacional de Notícias Árabes, 2024). O acordo assinado em 2024 com a administração do município prevê a cooperação nas áreas de tecnologia avançada, cidades inteligentes e investimentos voltados para o desenvolvimento de mão de obra qualificada (EDGE Group, 2024), deixando claro o interesse do grupo no desenvolvimento de redes de conhecimento e atração de cérebros brasileiros para seus projetos.

Assim, fica evidente que a atuação do EDGE vai muito além de contratos militares, buscando uma integração abrangente entre empresas privadas, governos estaduais e

instituições de pesquisa, ampliando sua influência em setores chave da tecnologia brasileira. Esse movimento revela uma dinâmica de interdependência assimétrica, na qual, enquanto o Estado busca ampliar suas capacidades de defesa e segurança por meio de acordos firmados com empresas estrangeiras, estas direcionam seus investimentos visando o acesso a recursos estratégicos e a absorção do *know-how* necessário para o desenvolvimento dessas tecnologias. Nesse processo, funções que antes eram tradicionalmente estatais – como a gestão da segurança pública ou o desenvolvimento de armamentos – passam a ser compartilhadas e conduzidas por corporações privadas. Toda essa dinâmica reflete o pensamento desenvolvido por Nye e Keohane (1977) sobre a interdependência complexa, em que o poder deixa de ser monopólio exclusivo do Estado e passa a ser compartilhado com diversos atores globais, como empresas privadas de tecnologia e segurança.

A partir disso, o EDGE começa a voltar sua atenção para o setor de segurança pública estadual, utilizando São Paulo como vitrine tecnológica para suas soluções. Essa aproximação evidencia uma estratégia de atuação do grupo em que a lógica da defesa militar se expande para o policiamento urbano e a vigilância dos indivíduos. É nesse cenário que nasce o projeto “Bola de Cristal”, apresentado como um modelo de inovação tecnológica que, na prática, consolida um sistema de vigilância preditiva integrado às forças policiais do estado de São Paulo.

4.2 O projeto “Bola de Cristal”

O Bola de Cristal é um sistema de vigilância desenvolvido pela empresa árabe EDGE Group voltado para sistemas integrados de monitoramento urbano. Originalmente pensado para fins militares, o sistema vem sendo adaptado para que possa ser utilizado no contexto civil, sendo incorporado em políticas de segurança pública.

Desde a implementação do Detecta, até o desenvolvimento e aplicação do Muralha, em 2024, é possível observar um processo de ampliação e integração entre os sistemas de monitoramento, a inclusão das empresas privadas e o crescente monitoramento do cotidiano dos paulistas. Tais projetos buscam usar ferramentas de coleta massiva de dados para garantir políticas de segurança pública.

É nesse cenário que nasce uma parceria entre o EDGE e o Governo do Estado de São Paulo. Segundo a CNN Brasil (GARCIA, 2024), o grupo árabe firmou uma parceria com o governo de Tarcísio visando usar o estado como um laboratório para o uso de tecnologias preditivas de segurança na América Latina. Nasce então o “Bola de Cristal”, cujo investimento na época girava em torno de US\$15 milhões.

De acordo com o Metrôpoles (MARCUS, 2024), o sistema foi apresentado como uma tecnologia capaz de prevenir crimes antes de serem cometidos, realizando abordagens em pessoas com histórico criminal ou com “comportamentos suspeitos”. Diferentemente dos projetos antigos do estado, que exigiam câmeras de alta resolução e conexões em nuvem, qualquer câmera pode ser integrada ao sistema do Bola de Cristal. Segundo o major Eduardo Fernandes Gonçalves, as câmeras não precisam ter mecanismos de reconhecimento facial, nem alta resolução, o próprio software do EDGE será responsável por implementar tais mecanismos.

Ainda, visando aumentar sua atuação, o projeto busca integrar o software às câmeras de vigilância corporais dos policiais. Dessa forma, o monitoramento não estaria restrito apenas aos ambientes públicos, como praças, terminais rodoviários, ruas, instituições, ou privados, como empresas, residências e condomínios, mas também estaria acoplado diretamente às forças policiais.

Na prática, o sistema é apresentado como uma inovação tecnológica capaz de identificar suspeitos, localizar desaparecidos, rastrear veículos em tempo real e prevenir crimes. Contudo, opera como um modelo de policiamento preditivo abastecido por dados do cotidiano que são usados para orientar decisões operacionais. Assim, o espaço urbano passa a ser mediado por algoritmos que filtram, classificam e priorizam determinados comportamentos, reforçando padrões seletivos de vigilância (UNIFESP, 2024)

Em 2025, o Muralha Paulista – projeto que abriga o *Crystall Ball* – entrou em expansão, buscando maior adesão dos municípios do estado. De acordo com a Secretaria de Segurança Pública, mais de 500 cidades são esperadas para aderir ao projeto até o final do ano. Além disso, em setembro de 2025 o governo liberou um decreto estadual que deu início ao cadastramento de pessoas físicas e jurídicas que querem, voluntariamente, cadastrar suas câmeras para contribuir com o monitoramento no estado de São Paulo (SSP SP, 2025).

Essa expansão demonstra uma convergência entre os interesses públicos e privados a fim de criar uma infraestrutura de vigilância. Enquanto o governo do estado busca aumentar a eficiência policial, o EDGE fortalece sua influência comercial no Brasil e na América Latina. Assim, tal dinâmica ilustra o que Zuboff (2019) defende no capitalismo de vigilância, em que a segurança se torna uma forma de mercantilização de dados e experiências.

Ainda, como observa Peron e Alvarez (2021), o estado de São Paulo acaba se tornando um laboratório de testagem de tecnologias, no qual a segurança pública se torna um produto atrativo para grandes empresas estrangeiras. A cidade, nesse sentido, exemplifica o modelo de “sociabilidade secundária” descrito pelos autores, em que há um compartilhamento no controle da vigilância entre o Estado e empresas de tecnologia. Assim, o Brasil acaba sendo inserido numa economia de vigilância, em que novas formas de governança são orientadas por dados e algoritmos.

Dessa forma, a experiência do estado de São Paulo com o projeto Bola de Cristal mostra como políticas de segurança têm servido de experimentação tecnológica, conectando os interesses públicos aos interesses das Big Techs. Tal dinâmica acaba revelando a inserção do Brasil em uma rede transnacional de vigilância, em que tecnologias estrangeiras passam a mediar o poder dos Estados. Logo, países como o Brasil passam a fazer parte de um ecossistema de coleta, processamento e compartilhamento de dados.

Diante disso, o próximo capítulo busca expandir, brevemente, a análise para o plano nacional e internacional, trazendo questões sobre a soberania digital e dependência tecnológica.

5. Soberania e Geopolítica dos Dados: O Brasil na Era da Vigilância Automatizada

A corrida por mercados consumidores de tecnologia, aliada à consolidação da inteligência artificial como um novo mecanismo de poder, ampliam disputas que vão além do campo tecnológico. O Brasil, inserido no sul global, ainda carece no que diz respeito à produção e ao domínio tecnológico, o que faz com que sua experiência com as inovações

tecnológicas seja complexa: ainda que se beneficie das inovações trazidas pela Quarta Revolução Industrial, torna-se também dependente de tecnologias estrangeiras.

Dessa forma, esse capítulo busca discutir as implicações geopolíticas do uso da vigilância automatizada, se atendo a três tópicos centrais: a dependência tecnológica brasileira, o papel do país no Sul Global e a atuação do país como território teste das tecnologias dos países desenvolvidos.

5.1 Dependência tecnológica e soberania digital

O avanço não apenas das tecnologias de vigilância, mas da inteligência artificial como um todo, expõe uma nova forma de dependência e colonização dos países do Sul Global em relação às grandes potências mundiais – detentoras do conhecimento e desenvolvimento tecnológico. No caso brasileiro, essa dependência fica evidente não apenas no que diz respeito à importação de equipamentos, mas também na terceirização do processamento e da análise dos dados coletados aqui.

Como já abordado anteriormente, o presidente da Google Brasil afirmou que “sem investimentos nacionais em inteligência artificial, o país corre risco de se tornar apenas um consumidor de tecnologia estrangeira, sem autonomia sobre seus dados e sistemas estratégicos” (VEJA, 2024). Essa declaração evidencia que, apesar do crescente uso de IA nos mais diversos setores, sejam eles públicos ou privados, o país ainda não detém controle sobre as plataformas que processam e armazenam as informações produzidas no país.

Zuboff (2019) mostra que os dados são elementos fundamentais para o funcionamento do capitalismo de vigilância, em que as experiências dos indivíduos são moldadas e usadas pelas empresas, desempenhando assim, papel de matéria-prima na acumulação de capital das Big Techs. Dessa forma, na economia global atual, os dados assumem papel de um recurso estratégico, fundamental para a manutenção de poder e influência.

Essa lógica contribui para que haja um deslocamento no eixo de poder do Sistema Internacional, abrindo espaço para o que Morozov (2013) chama de solucionismo tecnológico, em que a sociedade acredita que a tecnologia é capaz de solucionar problemas sociais, políticos e humanos, independente da sua complexidade. No entanto,

tal ideia ignora diversas questões estruturais – como a desigualdade, a pobreza, a violência –, históricas, culturais e políticas, resumindo tudo à algoritmos e sistemas. Morozov alerta que a adoção desenfreada e acrítica das tecnologias aprofunda assimetrias de poder e fragiliza a autonomia nacional.

Ao ceder o controle das estruturas digitais a companhias estrangeiras, os Estados transferem parte da sua capacidade decisória. Dessa forma, as decisões não necessariamente estarão alinhadas com os interesses públicos, mas sim aos interesses econômicos dessas empresas. No entanto, é preciso relativizar essa distinção: até que ponto o controle e o uso dos dados configuram uma questão de interesse público, e onde começam os interesses corporativos e privados? Em muitos casos, o discurso da inovação tecnológica é utilizado tanto pelo Estado quanto pelas empresas para justificar a necessidade da prática de coleta e uso de dados, tornando porosa a distinção entre interesses de grupos econômicos e aquilo que é promoção do bem comum, ao mesmo tempo, acabam reforçando lógicas de mercado e de uma vigilância que reforça desigualdades sociais. Ainda, países como o Brasil permanecem na posição de fornecedores de dados e consumidores de tecnologia, confirmando assim o colonialismo de dados exposto por Couldry e Mejias (2019).

Essa nova configuração deixa evidente que a soberania na era digital não se define mais apenas pelo controle territorial ou militar, mas também pela capacidade que um Estado possui de gerir suas informações e proteger suas infraestruturas tecnológicas. Dessa forma, o controle de dados torna-se um ator central do poder na atualidade.

5.2 O Brasil e a reconfiguração do poder no Sul Global

A atual corrida por tecnologias tem revelado uma nova disputa por poder, na qual o domínio sobre a inteligência artificial e o controle de dados define vantagens econômicas, políticas e estratégicas. Segundo análise publicada por O Globo (2025), o mundo está se dividindo entre países detentores de tecnologias avançadas e aqueles que dependem de soluções estrangeiras. Apenas 32 países possuem centros de dados especializados em IA, sendo que a maioria deles está localizada nos Estados Unidos, China e União Europeia. Ainda, empresas norte-americanas e chinesas controlam mais de 90% dos data centers,

demonstrando, portanto, a extrema concentração de poder digital nas mãos de poucos Estados.

Além dos dados, a corrida por tecnologia e os investimentos bilionários de algumas empresas também reforçam essas assimetrias. Segundo a Forbes, acordos bilionários entre as gigantes da tecnologia, OpenAI e Nvidia – com investimentos de 100 bilhões de dólares – mostram uma intensificação da capacidade de processamento e desenvolvimento de novos modelos. Ainda, mostra a formação de blocos hegemônicos formados pelas Big Techs em busca de controle de setores de tecnologia. Essa dinâmica acaba barrando países que não dispõem de infraestrutura e capital elevado, ampliando assim a divisão entre produtores e consumidores de tecnologia – norte e sul global, respectivamente.

O Brasil por sua vez desempenha um papel ambíguo nessa corrida. Ainda que se destaque no que diz respeito à América Latina, ainda depende da importação de tecnologias e parcerias com empresas estrangeiras para desenvolver seus próprios sistemas. Essa lacuna tecnológica cria o cenário ideal para que corporações estrangeiras influenciem políticas públicas e direcionam recursos estratégicos em áreas como segurança e defesa.

Um exemplo disso é o acordo firmado entre o governo brasileiro e os Emirados Árabes Unidos, em 2024, para a implementação de tecnologias de vigilância voltadas ao combate a crimes ambientais e ao monitoramento das fronteiras na Amazônia (GARCIA, 2025). Embora o projeto se apresente como uma cooperação estratégica, ele também expõe o interesse geopolítico das potências tecnológicas – como os Emirados e a China – em ampliar a sua influência sobre o território e os dados brasileiros.

Retomando o pensamento de Peron e Alvarez (2021), cidades como São Paulo se tornam laboratórios para a testagem de modelos de segurança, onde são testados modelos de segurança importados. A atuação de empresas como o EDGE Group confirma essa tendência: o Brasil é visto não apenas como mercado consumidor, mas como porta de entrada para o mercado latino-americano, funcionando como vitrine e meio de expansão regional.

Essa nova dinâmica transforma, portanto, o Sul Global em área de interesse tecnológico, em que dados, indivíduos e seus comportamentos são monitorados, categorizados e moldados de acordo com algoritmos desenvolvidos pelo Norte Global. Assim, fica evidente uma assimetria estrutural: enquanto poucos países produzem,

controlam e manipulam tecnologias, a maioria apenas as consome e se submete às suas lógicas. Se conformando como uma área de duplo extrativismo: ao mesmo tempo, são os principais fornecedores de minerais necessários para produção das tecnologias, e sua população torna-se base de dados matéria-prima para o desenvolvimento de algoritmos e modelos de aprendizagem que serão usados nos produtos comerciais dessas empresas estrangeiras.

6. Considerações Finais

Ao longo deste trabalho, buscou-se compreender as implicações geopolíticas do emprego da inteligência artificial em cenários de segurança, especialmente no contexto brasileiro. Para tanto, partiu-se do entendimento de que a inteligência artificial não é apenas uma ferramenta tecnológica, mas se configura como um instrumento de poder político e econômico. Assim, foi possível observar como sua utilização em políticas de segurança pública tem transformado as relações entre o Estado, a tecnologia e a sociedade.

Nos capítulos iniciais, discutiu-se a Quarta Revolução Industrial e como as tecnologias atuais, como a inteligência artificial, passam a ocupar papel de destaque na administração pública e na segurança. Buscou-se argumentar que a IA, ao ser apresentada como solução para a resolução de problemas complexos, aprofunda a crença no chamado solucionismo tecnológico, conforme alerta Morozov (2013). Tais crenças mascaram as dimensões políticas, sociais e históricas dos problemas, reduzindo-os à atuação de algoritmos.

Em seguida, foi realizada uma análise do estado de São Paulo como laboratório de políticas de segurança e como projetos de vigilância, como o Bola de Cristal, extrapolam o campo da segurança e são usados como ferramentas de controle social. A parceria firmada entre o governo do estado e o conglomerado de defesa EDGE Group mostra uma crescente interdependência entre o setor público e privado, sendo que o fornecimento de novas tecnologias influencia diretamente nas prioridades e decisões governamentais. Ainda, essa dinâmica viabiliza o que Peron e Alvarez chamam de sociabilidade securitária, em que os cidadãos, as empresas e o Estado passam a compartilhar a responsabilidade da vigilância.

Ao ampliar a análise para o cenário internacional, foi possível notar a ambiguidade da atuação brasileira frente à corrida tecnológica. Ainda que o país desempenhe certo destaque regionalmente, buscando modernizar suas estruturas e investir em inovação, permanece dependente de tecnologias e infraestruturas estrangeiras, comprometendo sua soberania digital. Essa dependência não é apenas técnica, mas também política, visto que os interesses das grandes empresas passam a influenciar decisões estratégicas e condicionar resoluções de acordo com seus interesses.

Nesse sentido, Zuboff (2019) ajuda na compreensão de como o capitalismo de vigilância transforma os dados pessoais e as experiências humanas em matéria prima para acumulação de poder econômico e tecnológico. Assim, quanto mais os Estados e suas instituições se apoiam em tecnologias privadas de gestão de segurança pública, mais se consolidam relações de dependência e transferência de poder. Logo, o conceito de colonialismo de dados abordado por Couldry e Mejias (2019) representa uma nova forma de exploração em que os países do sul global, extremamente dependentes da tecnologia do norte, alimentam sistemas de poder das grandes empresas de tecnologia.

Por fim, diante de todo o contexto apresentado, é possível notar que o emprego da inteligência artificial no cenário brasileiro demonstra tanto a busca por maior eficiência e modernização quanto um modelo de vigilância automatizada que amplia o poder das *Big Techs*. Ao importar estruturas tecnológicas e terceirizar o processamento dos seus dados, acaba reforçando estruturas de dependência que comprometem sua autonomia.

Diante desse cenário, compreender as implicações do uso da inteligência artificial na segurança pública ajuda a compreender as mudanças nas formas de poder e controle atuais. O Brasil, na tentativa de se modernizar, acaba expondo contradições entre inovação e dependência. Nesse sentido, além de pensar no futuro da segurança pública, deve-se também pensar sobre quem controla os mecanismos de vigilância e os dados coletados.

REFERÊNCIAS

AGÊNCIA NACIONAL DE NOTÍCIAS ÁRABES. **EDGE Group faz parceria com São José dos Campos**. ANBA, 19 ago. 2024. Disponível em: <https://anba.com.br/edge-group-faz-parceria-com-sao-jose-dos-campos/>. Acesso em : 18 jul. 2025.

AMARAL, Isabelle. **‘Iniciativa que traz esperança’, diz 1º empresário a cadastrar**

câmeras no Muralha Paulista. Secretaria de Segurança Pública de São Paulo, 11 nov. 2025. Disponível em: <https://www.ssp.sp.gov.br/noticia/59433>. Acesso em 10 out. 2025.

ARAÚJO, Matheus; VESPA, Talyta. ***Reconhecimento facial de SP confunde idoso com estuprador foragido.*** UOL, 13 abr. 2025. Disponível em: <https://noticias.uol.com.br/cotidiano/ultimas-noticias/2025/04/13/reconhecimento-facial-de-s-p-confunde-idoso-com-estuprador-foragido.htm>. Acesso em: 23 jun 2025.

AUGUSTO, Thaís. **SP lança edital para sistema de câmeras que identifica cor e 'vadiagem'.** UOL, 28 nov. 2022. Disponível em: <https://noticias.uol.com.br/cotidiano/ultimas-noticias/2022/11/28/sp-lanca-edital-para-sistema-de-cameras-que-identifica-cor-e-vadiagem.htm>. Acesso em: 23 jun 2025.

BARROS, Camila. **O país se digitaliza: o avanço e os desafios do setor de tecnologia no Brasil.** Veja Negócios, 14 set 2024. Disponível em: https://veja.abril.com.br/economia/o-pais-se-digitaliza-o-avanco-e-os-desafios-do-setor-de-tecnologia-no-brasil/#google_vignette. Acesso em: 23 jun 2025.

BBC News Brasil. **Apple vale US\$ 2 tri: valor de empresa nascida em garagem já é maior que PIB de 95% dos países.** Disponível em: <https://www.bbc.com/portuguese/internacional-53847955>. Acesso em: 14 jul 2025.

BIGO, Didier. **Security and Immigration: Toward a Critique of the Governmentality of Unease.** *Alternatives: Global, Local, Political*, v. 27, n. 1, p. 63-92, 2002.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

CORMEN, Thomas H. **Algoritmos: teoria e prática.** 3. ed. Rio de Janeiro: Elsevier, 2009.

COULDRY, Nick; MEJIAS, Ulises A. **The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism.** Stanford: Stanford University Press, 2019.

DAE Jundiaí. **DAE busca inteligência artificial para controle de perdas.** Dae Jundiaí, 04 jul. 2024. Disponível em: <https://daejudiai.com.br/2024/07/dae-busca-inteligencia-artificial-para-controle-de-perdas/>

DIAS, Tatiana. **Ofensiva das big techs contra PL das Fake News expõe lobby mais poderoso do mundo.** The Intercept, 8 maio 2023. Disponível em: <https://www.intercept.com.br/2023/05/08/pl-das-fake-news-big-techs-tem-maior-lobby-do-mundo>. Acesso em: 3 jun 2025.

BITENCOUT, K. **Importações de Tecnologia Crescem 15% e Impulsionam Inovação no Brasil.** Efficienza, 12 ago. 2025. Disponível em: <https://efficienza.com.br/importacoes-de-tecnologia-crescem-15-e-impulsionam-inovacao-no-brasil/>. Acesso em: 27 ago. 2025.

EDGE Group. **EDGE Group to Partner with the São Paulo State Government on Major Public Security Initiative.** Disponível em:

<https://edgegroupuae.com/news/edge-group-partner-sao-paulo-state-government-major-public-security-initiative>. Acesso em: 18 jul. 2025.

EDGE Group. **EDGE Group Signs Cooperation Agreement with the Government of São José dos Campos**. Disponível em:

<https://edgegroupuae.com/news/edge-group-signs-cooperation-agreement-government-sao-jose-dos-campos>. Acesso em: 18 jul. 2025.

EDGE Group. **EDGE and AKAER Sign MoU to Enhance Cooperation in Technology and Defence**. Disponível em:

<https://www.etimad.ae/news/edge-and-akaer-sign-mou-enhance-cooperation-technology-and-defence>. Acesso em 18 jul. 2025.

EDGE Group. **EDGE Strengthens Ties with the Sao Paulo State Government, Paving the Way for Significant Growth**. Disponível em:

<https://edgegroupuae.com/news/edge-strengthens-ties-sao-paulo-state-government-paving-way-significant-growth>. Acesso em: 18 jul. 2025.

EDGE Group. **EDGE Signs MoU with Brazil's SIATT at LAAD 2023**. Disponível em:

<https://edgegroupuae.com/news/edge-signs-mou-brazils-siatt-laad-2023>. Acesso em: 18 jul. 2025.

EDGE Group. **EDGE Group and the São Paulo State Government Sign Comprehensive Partnership Agreement**. Disponível em:

<https://edgegroupuae.com/news/edge-group-and-sao-paulo-state-government-sign-comprehensive-partnership-agreement>. Acesso em: 18 jul. 2025.

EDGE Group. **EDGE to Open LATAM Regional Office in Brazil**. Disponível em:

<https://edgegroupuae.com/news/edge-open-latam-regional-office-brazil>. Acesso em: 18 jul. 2025.

EDGE Group. **EDGE Group Receives High Level Delegation from the Sao Paulo State Government**. Disponível em:

<https://edgegroupuae.com/news/edge-group-receives-high-level-delegation-sao-paulo-state-government>. Acesso em: 18 jul. 2025.

ESTADÃO. **Edge Group, gigante do setor militar dos Emirados Árabes, compra segunda empresa no Brasil**. UOL, 30 abr. 2024. Disponível em:

<https://noticias.uol.com.br/ultimas-noticias/agencia-estado/2024/04/30/edge-group-gigante-do-setor-militar-dos-emirados-arabes-compra-segunda-empresa-no-brasil.htm>. Acesso em: 18 jul. 2025

ESTADÃO CONTEÚDO. **“Venda de íris” continua proibida no Brasil após empresa tenta driblar veto da ANPD**. InfoMoney, 06 ago. 2025. Disponível em:

<<https://www.infomoney.com.br/brasil/venda-de-iris-continua-proibida-no-brasil-apos-empresa-tenta-driblar-veto-da-anpd/>>. Acesso em: 3 nov. 2025.

FOUCAULT, Michel. **Segurança, território, população**: curso no Collège de France (1977–1978). São Paulo: Martins Fontes, 2008.

FREITAS, Caio; VALENTE, Rubens. **Projeto de vigilância de Tarcísio em São Paulo partiu do Córtex, do Governo Federal**. Pública, 14 out. 2024. Disponível em: <https://apublica.org/2024/10/muralha-paulista-o-projeto-de-vigilancia-de-tarcisio-em-sp/>. Acesso em: 9 jun 2025.

FREITAS, Caio; VALENTE, Rubens. **Ministério da Justiça não quis auditar o uso do Córtex pelo governo Bolsonaro**. Pública, 12 out. 2024. Disponível em: <https://apublica.org/2024/10/cortex-mj-nao-quis-auditar-sistema-espiao-pelo-governo-bolsonaro/>. Acesso em: 9 jun 2025.

FROM THE NEWSROOM. **UAE's EDGE Group prepares acquisitions in Brazil**. ANBA News Agency, 28 mar. 2024. Disponível em: <https://anba.com.br/en/uaes-edge-group-prepares-acquisitions-in-brazil/>. Acesso em: 18 jul. 2025.

GALISI, Juliano. **Senado Federal compra programa de reconhecimento facial Clearview AI em possível afronta à Lei Geral de Proteção de Dados**. *Estadão*, São Paulo. Disponível em: <https://www.estadao.com.br/politica/senado-federal-compra-programa-reconhecimento-facial-clearview-ai-lei-geral-protecao-dados-nprp/>. Acesso em: 09 jul. 2025.

GALVANI, Giovanna. **90% das pessoas presas por reconhecimento facial são negras, diz estudo**. CESeC, 22 nov. 2019. Disponível em: <https://cesecseguranca.com.br/reportagens/90-das-pessoas-presas-por-reconhecimento-facial-sao-negras-diz-estudo/>. Acesso em: 09 jul. 2025.

GARCIA, Gabriel. **Após investimentos de R\$ 3 bi, Grupo Edge vai construir duas fábricas no Brasil**. CNN Brasil, 06 jan. 2025. Disponível em: <https://www.cnnbrasil.com.br/economia/negocios/apos-investimentos-de-r-3-bi-grupo-edge-vai-construir-duas-fabricas-no-brasil/>. Acesso em: 09 jul. 2025.

GARCIA, Gabriel. **Edge Group firma parceria com governo de São Paulo para uso de IA na segurança pública**. CNN Brasil, Brasília, 18 jan. 2024. Disponível em: <https://www.cnnbrasil.com.br/politica/governo-de-sp-e-empresa-dos-emirados-arabes-faz-m-parceria-para-combater-criminalidade-com-o-uso-de-inteligencia-artificial/>. Acesso em: 10 maio 2025.

GULFTODAY. **EDGE announces acquisition of 50% stake in Brazil's SIATT**. Disponível em: <https://www.gulftoday.ae/business/2023/09/29/edge-announces-acquisition-of--50-stake-in-brazils-siatt>. Acesso em: 18 jul. 2025.

HENRIQUE, Alfredo. **Smart Sampa é induzido ao erro e indica PM fardado como foragido**. METRÓPOLES, 19 março 2025. Disponível em: <https://www.metropoles.com/sao-paulo/smart-sampa-e-induzido-ao-erro-e-indica-pm-fardado-como-foragido>. Acesso em: 10 out. 2025.

KEOHANE, Robert O.; NYE, Joseph S. **Power and Interdependence: World Politics in Transition**. Boston: Little, Brown and Company, 1977.

INTERCEPT BRASIL. **Ministério da Justiça comprou secretamente tecnologia que coleta fotos sem autorização para reconhecimento facial.** *The Intercept Brasil*, São Paulo, 3 fev. 2025. Disponível em: <https://www.intercept.com.br/2025/02/03/ministerio-da-justica-comprou-secretamente-tecnologia-que-coleta-fotos-sem-autorizacao-para-reconhecimento-facial/>. Acesso em: 09 jul. 2025.

LASINTEC. **Uma muralha invisível:** Controles a céu aberto, monitoramentos e polícia preditiva. Universidade Federal de São Paulo, 2024. Disponível em: <https://lasintec.unifesp.br/boletins/boletins-antiseuran%C3%A7a/40-boletim-antiseuran%C3%A7a>. Acesso em: 8 set. 2025.

MARCUS, Enzo. **Como funcionará o “Big Brother”, projeto de vigilância do estado de SP.** *Metrópoles*, 27 jul. 2024. Disponível em: <https://www.metropoles.com/sao-paulo/como-funcionara-o-big-brother-projeto-de-vigilancia-do-estado-de-sp>. Acesso em: 14 ago. 2025.

MARINHA DO BRASIL. **Acordo com EDGE Group assinado com Corpo de Fuzileiros Navais do Brasil para desenvolvimento de veículos autônomos e guerra eletrônica.** Rio de Janeiro, 23 nov. 2023. X: @marmilbr. Disponível em: <https://x.com/marmilbr/status/1707048402284863802>. Acesso em: 1 nov. 2025.

MARTINS, Lais. **14 fotos por ser humano.** INTERCEPT BRASIL, 16 maio 2023. Disponível em: <https://www.intercept.com.br/2023/05/16/em-reunioes-secretas-clearview-policias-ministerio-da-justica/>. Acesso em: 09 jul. 2025.

McCARTHY, John et al. **A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence.** 1955. Disponível em: <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>.

MEDEIROS, H. **Prefeitura de São Paulo instalará 20 mil câmeras com reconhecimento facial.** *Mobile Time*, 07 ago. 2023 Disponível em: <https://www.mobiletime.com.br/noticias/07/08/2023/prefeitura-de-sao-paulo-instalara-20-mil-cameras-com-reconhecimento-facial>. Acesso em: 15 jul. 2025.

MELLO, Daniel. **São Paulo avança em integração de sistemas de hipervigilância.** AGÊNCIA BRASIL, 27 jan. 2024. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2024-01/sao-paulo-avanca-em-integracao-de-sistemas-de-hipervigilancia>. Acesso em: 09 jul. 2025.

MONUV. **Smart Sampa:** prefeitura de São Paulo – SP. 2024. Disponível em: <https://suporte.monuv.com.br/pt-BR/articles/9636114-smart-sampa-prefeitura-de-sao-paulo-sp>. Acesso em: 20 jun. 2025.

MONUV. **Detecta - Polícia Militar de SP.** Disponível em: <https://suporte.monuv.com.br/pt-BR/articles/9636107-detecta-policia-militar-de-sp> Acesso em: 20 jun. 2025.

MORENO, Ana Carolina. **Edge Group, dos Emirados Árabes, investe no Brasil para criar ‘nova Embraer’, de mísseis.** InvestNews, 17 mar. 2025. Disponível em: <https://investnews.com.br/negocios/edge-group-dos-emirados-arabes-investe-no-brasil-para-criar-uma-nova-embraer-de-misseis/> Acesso em: 23 jun. 2025.

MOURA, Matheus; COELHO, Leonardo. **Reconhecimento policial:** sem protocolo, polícias do Rio usam câmeras e cometem erros. Publica, 14 jun 2024. Disponível em: <https://apublica.org/2024/06/reconhecimento-policial-sem-protocolo-policias-do-rio-usam-cameras-e-cometem-erros/>. Acesso em: 09 jul. 2025.

O GLOBO. **Corrida pela IA provoca nova divisão no mundo: os que têm acesso à tecnologia e os que não têm.** Disponível em: <https://oglobo.globo.com/economia/tecnologia/noticia/2025/06/24/corrida-da-ia-esta-dividindo-o-mundo-entre-os-que-tem-sistemas-avancados-e-os-que-nao-tem.ghtml>. Acesso em: 02 out. 2025.

PANTALEÃO, Bruno; NUNES, Pablo. **Smart Sampa vigia, mas não protege:** falta de evidência na redução de crimes e aumento da produtividade policial na cidade de São Paulo. Rio de Janeiro: CESeC, 2025.

PATI, Camila. **‘O limite da IA é a nossa criatividade’, diz presidente do Google Brasil.** VEJA Negócios, 26 set. 2025. Disponível em: <https://veja.abril.com.br/economia/o-limite-da-ia-e-a-nossa-criatividade-diz-presidente-do-google-brasil/>. Acesso em: 30 set. 2025

PAULO, V. S. **Empresa dá lance de R\$9,2 milhões por mês para implementar Smart Sampa.** Veja São Paulo, 28 mai. 2023. Disponível em: <https://veja.abril.com.br/cidades/empresa-da-lance-de-r-92-milhoes-por-mes-para-implementar-smart-sampa>. Acesso em: 30 set. 2025.

PERON, Alcides. **Tecnologia de vigilância pode reproduzir violência presente na própria sociedade.** Jornal da USP, 13 set. 2022. Disponível em: <https://jornal.usp.br/atualidades/tecnologia-de-vigilancia-pode-reproduzir-violencia-presente-na-propria-sociedade/>. Acesso em: 30 set. 2025

PERON, Alcides; ALVAREZ, Marcos. **O Governo da Segurança:** Modelos securitários transnacionais e tecnologias de vigilância na cidade de São Paulo. Lua Nova, set. 2021. Disponível em: <https://www.scielo.br/lua/a/g6JndBVLsFhTBvBhmhMrYsb/?lang=pt>. Acesso em: 30 set. 2025

Peron, A.; Röhe, A. **Silenciamento sociotécnico e os limites do “poder instrumental”.** Instituto de Estudos Avançados da Universidade de São Paulo, 2024. Disponível em: <https://www.scielo.br/iea/a/yxzqzQ4CvXRz7VnZzGHdcQc/?format=html&lang=pt>. Acesso em: 4 nov. 2025.

PREFEITURA DE SÃO PAULO. **Prefeitura inaugura Prisômetro:** painel do Smart Sampa no centro da cidade. Prefeitura de São Paulo, 2024. Disponível em: <https://prefeitura.sp.gov.br/w/prefeitura-inaugura-pris%C3%B4metro-painel-do-smart-sampa>

-no-centro-da-cidade-com-n%C3%B3s-de-foragidos-capturados-presos-em-flagrante-e-pessoas-encontradas. Acesso em: 9 jun. 2025

PREFEITURA DE SÃO PAULO. **Site City Câmeras**. Prefeitura de São Paulo, 11 jul. 2017. Disponível em: https://prefeitura.sp.gov.br/web/seguranca_urbana/w/noticias/237446. Acesso em: 30 set. 2025

PREFEITURA DE SÃO PAULO. **Prefeitura de SP lança projeto City Câmeras**. Prefeitura de São Paulo, 2017. Disponível em: <https://prefeitura.sp.gov.br/w/noticia/prefeitura-de-sp-lanca-projeto-city-cameras>. Acesso em: 9 jun 2025.

PREFEITURA DE SÃO PAULO. **Legislação Municipal - DECRETO Nº 63.552 de 4 de Julho de 2024**. Disponível em: <https://legislacao.prefeitura.sp.gov.br/leis/decreto-63552-de-4-de-julho-de-2024/consolidado>. Acesso em: 9 jun. 2025.

QUINTELLA, Sérgio. **Alvo de críticas, projeto City Câmeras registra pouca adesão da população**. Veja São Paulo, 17 set 2021. Disponível em: <https://vejasp.abril.com.br/coluna/poder-sp/alvo-de-criticas-projeto-city-cameras-registra-pouca-adesao-da-populacao/> Acesso em: 9 jun. 2025

RIBEIRO, Bruno. **Exclusivo: conheça o sistema de monitoramento por câmeras de Tarcísio**. Metrôpoles, 28 jan. 2024. Disponível em: <https://www.metropoles.com/sao-paulo/exclusivo-o-pacote-que-tarcisio-planeja-contrar-criar-da-seguranca>

RIBEIRO, Bruno; RESK, Felipe. **O que se sabe da “Bola de Cristal” do crime, proposta árabe a Tarcísio**. Metrôpoles, 14 mai. 2024. Disponível em: <https://www.metropoles.com/sao-paulo/bola-de-cristal-crime-arabe-tarcisio>

RUSSELL, Stuart; NORVIG, Peter. **Artificial Intelligence: A Modern Approach**. 3. ed. Upper Saddle River: Prentice Hall, 2013.

SÃO PAULO (Estado). Polícia Militar. **Plano de Policiamento Inteligente**. São Paulo: PM, 2007

SECRETARIA DA SEGURANÇA PÚBLICA. **Programa Muralha Paulista**: Política pública de controle da mobilidade criminal. 2024. Disponível em: <https://www.muralhapaulista.sp.gov.br/institucional/sobre-o-muralha-paulista>. Acesso em: 15 set. 2025.

SECRETARIA DA SEGURANÇA PÚBLICA. **Detecta**: Cinturão eletrônico de videomonitoramento. Disponível em: <https://www.ssp.sp.gov.br/midia/Midia/00000262.pdf> Acesso em: 30 jul. 2025

SECRETARIA DA SEGURANÇA PÚBLICA. **Cartilha de adesão ao sistema Detecta - v3.0**. 2017. Disponível em: http://www.sapp.org.br/sapp/wp-content/uploads/Sistema_Detecta_cartilha_completa_v3.pdf

f. Acesso em: 30 jul. 2025

SETOR público gasta bilhões com tecnologia estrangeira ao invés de investir em ciência nacional. **Jornal da USP**, 14 jul. 2025. Disponível em: [Setor público gasta bilhões com tecnologia estrangeira ao invés de investir em ciência nacional – Jornal da USP](#). Acesso em: 31 out. 2025.

SILVA, E. C. M.; ROCHA, I.; VAZ, J. C.; VENEZIANI, J. R. A.; MODANEZ, C. C..
Contratos, Códigos e Controle: A Influência das Big Techs no Estado Brasileiro.
São Paulo - SP, Brasil, jul. 2025. Acesso em: <https://bit.ly/contratos-big-techs>

SOUSA, Bruno. **Panóptico**: reconhecimento facial renova velhas táticas racistas de encarceramento. Rede de Observatórios da Segurança, 22 abr. 2021. Disponível em: <https://observatorioseguranca.com.br/panoptico-reconhecimento-facial-renova-velhas-taticas-s-racistas-de-encarceramento/> Acesso em: 30 set. 2025

SZKURNIK, Iona. **ChatGPT acelera Corrida Global da IA**. Forbes, 02 out. 2025.
Disponível em: <https://forbes.com.br/colunas/2025/10/chatgpt-acelera-corrida-global-da-ia/>.
Acesso em 03 out. 2025.

WACQUANT, Loïc. **Punir os pobres**: a nova gestão da miséria nos Estados Unidos. Rio de Janeiro: Revan, 2003.

World Press & Media Center | World. Disponível em:
<https://world.org/pt-br/press>. Acesso em: 3 nov. 2025.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2019.