Legitimação Legislativa de Vigilância em Massa: Riscos à Democracia, Ciberdemocracia e à Liberdade Pública

Cauê Rodrigues de Aguiar[1]

Lis Loureiro Souza[2]

Rodolpho Raphael de Oliveira Santos[3]

Resumo

O artigo analisa a vigilância em massa como um dos principais mecanismos de regulação social na contemporaneidade, articulando o panóptico de Bentham às formulações foucaultianas sobre disciplina e biopoder para compreender a internalização do controle. Demonstra-se que tecnologias como câmeras de vigilância, reconhecimento facial, rastreamento de dispositivos móveis, monitoramento de comunicações, Internet das Coisas (IoT) e grandes bases de dados ampliam significativamente a capacidade de observação estatal e corporativa, produzindo impactos diretos sobre a privacidade, a autonomia individual e as liberdades públicas. A pesquisa realiza uma análise comparativa entre os modelos legislativos da China, dos Estados Unidos e do Brasil, identificando, respectivamente, um regime de controle estatal soberano, um capitalismo de vigilância fragmentado e um arranjo híbrido marcado por disputas normativas. Sustenta-se que, embora legitimadas por discursos de segurança, eficiência ou estabilidade social, essas práticas contribuem para a normalização da vigilância em massa e representam riscos estruturais à democracia. Por fim, defende-se a necessidade de marcos regulatórios robustos, transparência institucional e participação social na definição dos limites da vigilância tecnológica.

Palavras-chave: Vigilância; Controle social; Biopoder; Tecnologias de vigilância; Legislação.

Abstract

This article analyzes mass surveillance as one of the main mechanisms of social regulation in contemporary society, articulating Bentham's panopticon with Foucault's

[1] Graduando, Universidade Estadual do Sudoeste da Bahia, Membro do Núcleo de Pesquisa e Estudos Legislativos da Escola do Legislativo da Paraíba – ELEGIS – PB. E-mail: cauero@hotmail.com

[2] Graduanda, Fasavic Afya. E-mail: lisloureiro.sousa@gmail.com

[3] Mestre em Computação, Comunicação e Artes com linha de Pesquisa em Mídias em Ambientes Digitais pela Universidade Federal da Paraíba, UFPB, João Pessoa. Pós-Graduado em Administração Pública pela Faculdade Alffa do Brasil; Mídias Digitais, Comunicação e Mercado pelo Centro de Educação Superior Reinaldo Ramos, CESREI, Didática no Ensino Superior (FMU – Centro Universitário das Faculdades Metropolitanas Unidas); ABA – Análise do Comportamento Aplicada pela Faculdade Conexão, Belo Horizonte; Bacharel em Comunicação Social (Universidade Estadual da Paraíba, UEPB; Bacharel e Licenciado em Filosofia; Bacharel em Administração pela FAMAR; Bacharel em Teologia e Licenciado em História pela Uninter Centro Universitário. Coordenador do Núcleo de Pesquisa e Estudos Legislativos da Escola do Legislativo da Paraíba – ELEGIS – PB. E-mail: rprofessorpb@gmail.com

formulations on discipline and biopower to understand the internalization of control. It demonstrates that technologies such as surveillance cameras, facial recognition, mobile device tracking, communications monitoring, the Internet of Things (IoT), and large databases significantly expand the capacity for state and corporate observation, producing direct impacts on privacy, individual autonomy, and public freedoms. The research conducts a comparative analysis between the legislative models of China, the United States, and Brazil, identifying, respectively, a sovereign state control regime, a fragmented surveillance capitalism, and a hybrid arrangement marked by normative disputes. It argues that, although legitimized by discourses of security, efficiency, or social stability, these practices contribute to the normalization of mass surveillance and represent structural risks to democracy. Finally, it defends the need for robust regulatory frameworks, institutional transparency, and social participation in defining the limits of technological surveillance.

Keywords: Surveillance; Social control; Biopower; Surveillance technologies; Legislation.

Introdução

A aparente estabilidade da vida em sociedade revela-se, em grande medida, como uma ilusão que encobre um processo contínuo e historicamente situado de regulação social. Longe de ser espontânea, a ordem social resulta de uma arquitetura invisível composta por mecanismos de normatização, vigilância e controle, cujo exame tem instigado a sociologia e a teoria política desde seus primórdios. Autores como Durkheim, Althusser, Foucault e Bourdieu forneceram aportes fundamentais para compreender como as instituições operam como instâncias centrais de reprodução da ordem vigente. Nesse quadro analítico, vigilância e controle social configuram-se como dimensões complementares: enquanto o controle se manifesta por meio da normatividade e da intervenção institucional, a vigilância atua como base informacional e condição de possibilidade desse processo (SIERRA; FREIRE, 2021).

Esse debate adquire novos contornos no contexto da ciberdemocracia. A promessa inicial de uma ágora digital, orientada à ampliação da participação cidadã e ao fortalecimento do debate público, foi progressivamente tensionada pela ascensão do chamado capitalismo de vigilância, no qual a interação online tende a servir menos ao empoderamento cívico e mais à coleta massiva de dados, à modulação comportamental e ao controle social (COSTA, 2024). A expansão das plataformas digitais, longe de neutralizar relações de poder, reconfigura-as em novas bases técnicas e normativas.

A genealogia da vigilância contemporânea remonta ao panóptico de Jeremy Bentham, concebido no século XVIII e posteriormente ressignificado por Michel Foucault como paradigma das sociedades disciplinares (GANDY, 1989). Em *Vigiar e Punir*, Foucault (1977) descreve a vigilância como mecanismo central do controle social moderno, destacando a transição de formas ostensivas de dominação para modalidades mais sutis, contínuas e internalizadas de exercício do poder. Esse movimento, que marca a passagem da sociedade do espetáculo para a sociedade da vigilância, intensifica-se na contemporaneidade com a proliferação de dispositivos tecnológicos de monitoramento incorporados ao cotidiano de bilhões de indivíduos.

Exemplos recentes evidenciam a centralidade e a atualidade desse fenômeno. Reportagem do jornal *The Guardian* revelou alegações sobre o uso, por instituições militares israelenses, de tecnologias em nuvem da Microsoft para práticas de vigilância em massa da população palestina, no contexto do conflito israelo-palestino (DAVIES; ABRAHAM, 2025). De modo semelhante, a Human Rights Watch (2023) denunciou a utilização, pelo governo chinês, de aplicativos móveis para monitorar e deter arbitrariamente muçulmanos na região de Xinjiang, consolidando sistemas estruturados de vigilância e repressão.

Nesse cenário, Gandy (1989) já advertia para a emergência de sistemas automáticos de vigilância capazes de escapar aos mecanismos tradicionais de controle jurídico, como ocorre de maneira emblemática nos Estados Unidos sob um modelo fragmentado de vigilância capitalista. A controvérsia central, contudo, não reside apenas na expansão dessas tecnologias, mas sobretudo em seus processos de legitimação política e jurídica. Sob o argumento da segurança pública, da eficiência administrativa ou da estabilidade social, Estados têm justificado a adoção de práticas de vigilância em massa, frequentemente desconsiderando os riscos éticos, sociais e democráticos associados à intensificação da intrusão na esfera privada (FONTES; LÜTGE, 2022).

É precisamente nesse ponto que se insere o presente estudo, ao investigar de que maneira a ação legislativa, no período compreendido entre 2020 e 2025, tem buscado legitimar o uso de tecnologias de vigilância em massa, bem como ao evidenciar os riscos de sua normalização como mecanismos autoritários de controle social sustentados por discursos de “segurança” e “eficiência” no contexto global.

A relevância da pesquisa reside em examinar, de forma articulada, a dimensão ética do rigor democrático e os impactos políticos dessas práticas. A adoção generalizada de sistemas tecnológicos de vigilância afeta amplos contingentes populacionais e pode produzir consequências duradouras e irreversíveis, especialmente quando empregada de modo abusivo ou opaco. Diante disso, torna-se imperativo ampliar o debate acadêmico e público sobre os limites da vigilância estatal, contribuindo para o fortalecimento da Ciência Política e para uma compreensão crítica dos desafios que essas práticas impõem às democracias contemporâneas.

1. Fundamentos teóricos da vigilância e do controle social

O surgimento dos mecanismos de vigilância na modernidade fundamenta-se no projeto do Panóptico, idealizado pelo filósofo Jeremy Bentham (2013). O modelo consistia em uma estrutura carcerária composta por um anel periférico de celas individuais e uma torre central de vigilância, a partir da qual um observador poderia ver o interior de todas as celas sem que os detentos soubessem se estavam sendo monitorados em determinado momento. Sua eficácia não dependia da vigilância contínua, mas da certeza permanente de sua possibilidade, convertendo o prisioneiro no principal agente de sua própria disciplina (BENTHAM, 2013; GANDY, 1989).

A partir desse modelo de poder, Michel Foucault desenvolveu sua teoria da sociedade disciplinar. Para o autor, o panoptismo não se limita a uma construção arquitetônica, mas constitui um diagrama de tecnologia de poder aplicável a diferentes instituições voltadas ao controle dos indivíduos. Seu objetivo não é apenas punir, mas treinar, otimizar e normalizar comportamentos, produzindo os chamados corpos dóceis, sujeitos moldados por técnicas disciplinares previsíveis e funcionalmente integrados às instituições sociais, por meio da gestão minuciosa de atividades, gestos, tempos e espaços. Nesse sentido, o projeto de Bentham exemplifica a análise foucaultiana segundo a qual a disciplina é uma anatomia política do detalhe (FOUCAULT, 1977, p. 139, tradução nossa).

Entretanto, o poder disciplinar exercido sobre o corpo individual constitui apenas uma das dimensões do que Foucault denominou biopoder. A outra face desse dispositivo corresponde à biopolítica, uma tecnologia de poder voltada não ao indivíduo isolado, mas à população enquanto totalidade. Seu objeto central é a gestão da vida

coletiva, expressa no controle das taxas de natalidade e mortalidade, na promoção da saúde pública e na otimização da longevidade. Nessa perspectiva, o Estado e suas instituições passam a administrar a vida do chamado corpo-espécie, estabelecendo normas e padrões destinados a produzir populações saudáveis e produtivas, de modo que o poder moderno opere simultaneamente em dois registros: a disciplina dos corpos individuais e a regulação das populações (NETO et al., 2007; FOUCAULT; BRANDÃO, 2008).

Essa estrutura de poder, analisada por Foucault (1977) na transição da sociedade do espetáculo para a sociedade da vigilância, encontra sua máxima expressão na era digital. Observa-se, nesse contexto, o predomínio de formas cada vez mais sutis, contínuas e internalizadas de dominação, aplicadas de maneira abrangente a populações inteiras. Esse novo cenário materializa-se por meio de tecnologias que permeiam o cotidiano, incorporando-se às práticas sociais e refletindo, ao mesmo tempo, as racionalidades políticas que as orientam.

É nesse quadro que Zuboff (2021) identifica a emergência do capitalismo de vigilância, entendido como uma lógica de acumulação que ultrapassa a exploração tradicional do trabalho ao apropriar-se da experiência humana em sua totalidade como matéria-prima. Segundo a autora, a extração massiva de dados, favorecida pela persistente insuficiência de marcos regulatórios, não se limita à previsão de comportamentos, mas atua ativamente em sua modulação, instaurando um regime de poder assimétrico orientado por interesses econômicos.

A vigilância em massa, frequentemente implementada sob o pretexto da segurança pública, suscita questões centrais relacionadas ao seu uso exacerbado e ao grau de intrusão na privacidade individual (FONTES; LÜTGE, 2022). Como ponderam Pompeu, Trindade e Sato (2024), vive-se uma era de complexa ambiguidade, na qual os benefícios das tecnologias digitais coexistem com efeitos deletérios sobre a autonomia, a liberdade e os direitos fundamentais. A opacidade dos sistemas algorítmicos e a ausência de mecanismos eficazes de auditoria tornam ainda mais urgente o debate acerca dos limites éticos da vigilância em massa, da reafirmação dos direitos humanos no ciberespaço e da criação de instrumentos de transparência capazes de submeter o poder tecnológico ao escrutínio democrático.

2. Tecnologias de vigilância em massa e seus riscos

Nas últimas décadas, a evolução das tecnologias da informação foi marcada por avanços significativos na velocidade de transferência de dados, no poder de processamento, nas técnicas de visualização e na capacidade de armazenamento. Nesse contexto, tais transformações ofereceram aos Estados e a atores privados oportunidades inéditas para ampliar suas capacidades de vigilância e coleta de inteligência, redefinindo os limites tradicionais do monitoramento social (LEMIEUX, 2018). As tecnologias de vigilância em massa mais difundidas podem ser agrupadas em diferentes subcategorias, entre as quais se destacam as seguintes.

3. Vigilância por vídeo

Também conhecida como Closed Circuit Television (CCTV), a vigilância por vídeo consiste em uma rede privada de monitoramento na qual as imagens captadas por câmeras são transmitidas para conjuntos específicos de monitores ou dispositivos de gravação. A característica central desse circuito fechado reside em sua natureza autocontida, uma vez que o sinal de vídeo não é difundido publicamente, mas restrito a uma rede controlada.

Ao longo do tempo, a CCTV evoluiu para plataformas integradas de controle inteligente e análise automatizada, incorporando funcionalidades como a detecção de movimento e a identificação da presença humana por meio do reconhecimento facial (NURHOPIPAH; HARJOKO, 2018). Essa evolução contribui para a normalização do olhar estatal no cotidiano e, do ponto de vista democrático, acarreta riscos associados à erosão da esfera pública enquanto espaço de livre expressão, anonimato e contestação política.

4. Reconhecimento facial

O reconhecimento facial constitui uma tecnologia biométrica destinada à identificação ou verificação de indivíduos a partir da comparação de padrões faciais extraídos de imagens digitais ou de quadros de vídeo com bancos de dados previamente constituídos. Seu processamento pode ocorrer tanto em tempo real, integrado a sistemas de CCTV, quanto de forma retrospectiva, por meio da análise de imagens e gravações armazenadas (SLOBOGIN; BRAYNE, 2022). Diferentemente da mera detecção

de rostos, essa tecnologia avança para a identificação individual, cruzando dados biométricos únicos, como a distância entre os olhos, o formato do maxilar e o contorno do nariz.

Embora frequentemente apresentada como tecnicamente precisa, todas as etapas do reconhecimento facial envolvem graus relevantes de subjetividade humana e técnica, o que impõe a necessidade de uma análise crítica de sua aplicação, especialmente em contextos sensíveis (SLOBOGIN; BRAYNE, 2022). Trata-se de uma tecnologia que não apenas observa, mas também identifica, cataloga e rastreia indivíduos, de modo que seus vieses algorítmicos ameaçam diretamente o princípio da isonomia, sobretudo em práticas discriminatórias direcionadas a minorias. No âmbito da ciberdemocracia, isso implica o enfraquecimento do anonimato protetivo, inibindo a participação em debates públicos online e a organização de movimentos sociais diante do temor de identificação e retaliação.

5. Rastreamento de celulares

O avanço das tecnologias digitais ampliou as possibilidades de monitoramento de cidadãos. Entre os mecanismos mais recorrentes, a vigilância móvel se destaca pela ubiquidade dos smartphones e pela capacidade de gerar informações detalhadas sobre a rotina dos usuários. A coleta e o armazenamento desses dados configuram uma prática de vigilância constante, pouco visível e, muitas vezes, fora do alcance de regulamentações eficazes. Nesse contexto, observa-se que diferentes estudos descrevem de forma contundente o alcance e os riscos associados a esse tipo de vigilância:

> "Cada minuto de cada dia, em todo o planeta, dezenas de empresas, em grande parte não regulamentadas e pouco fiscalizadas, registram os movimentos de dezenas de milhões de pessoas com telefones celulares e armazenam as informações em arquivos de dados gigantescos" (SLOBOGIN; BRAYNE, 2022 apud THOMPSON; WARZEL, 2022, p. 5, tradução nossa).

Todavia, percebe-se que a vigilância móvel não se restringe ao monitoramento técnico, visto que, a depender do uso dos dados coletados, pode envolver dimensões sociais e políticas que exigem maior atenção acadêmica e regulatória (STEWART, 2012). O dilema democrático aqui é a supressão do espaço para a deliberação íntima e a

organização autônoma, cuja privacidade é invadida, alicerce para que ocorra o desenvolvimento de um pensamento crítico e da oposição política.

6. Monitoramento de comunicações

Engloba um conjunto de práticas e tecnologias voltadas para a interceptação, monitoramento e análise de comunicações eletrônicas, sejam elas realizadas por meio de chamadas telefônicas, mensagens de texto, e-mails, redes sociais ou aplicativos de mensagens instantâneas (SLOBOGIN; BRAYNE, 2022). Esse tipo de vigilância, como sempre, a depender do uso dos dados coletados, pode gerar diferentes graus e tipos de impacto, como exemplo do caso citado na introdução da atual crise israelo-palestina (Human Rights Watch, 2023).

A interceptação de comunicações indiscriminada é um ataque direto à liberdade de expressão e do pensamento, dado que ao violar o sigilo da correspondência, o Estado invade a esfera privada, com riscos de autocensura de forma geral, tanto em questões de debate de ideias, quanto em posicionamentos políticos contrários.

7. Sensores de IoT e residências inteligentes

A Internet das Coisas (IoT) pode ser entendida como uma “rede de dispositivos físicos, veículos, eletrodomésticos e outros objetos materiais que possuem sensores, softwares e conectividade de rede integrados, permitindo a coleta e o compartilhamento de dados” (IBM, 2023, tradução nossa). Segundo Statista (2025), o número de dispositivos IoT conectados deverá ultrapassar 40 bilhões em 2034, com a maior concentração na região da Grande China, seguida pela Europa e América do Norte. O fenômeno da IoT revela implicações em termos sociais, econômicos e políticos, visto que vem, recentemente, criando novas oportunidades de vigilância em massa e revolucionando os métodos tradicionais de coleta de informações (LEMIEUX, 2018).

Esse tipo de vigilância representa a forma mais totalizante de controle, no qual o olhar panóptico está presente a todo momento, visto que erode a esfera íntima de modo a comprometer a capacidade do indivíduo de se desenvolver como um ser autônomo, uma das condições para existir uma cidadania democrática.

8. Utilização de dados públicos e compartilhados

Uma prática comum no mercado de dados é a coleta de informações a partir de fontes públicas para o seu reaproveitamento, somada à venda, por parte de empresas, de dados compartilhados por seus clientes. Essas informações podem ser utilizadas em análises comportamentais, como as realizadas pela Cambridge Analytica (CA) por meio da mineração de redes sociais. Especializada em "microdirecionamento psicográfico", a CA identifica traços específicos de públicos-alvo até o nível individual, consultando políticos sobre como customizar mensagens. Esse modelo foi amplamente utilizado em 2014; a empresa foi contratada por 44 campanhas políticas nos EUA, atuando depois nas bem-sucedidas campanhas de Ted Cruz e de Donald Trump em 2016 (Underwood; Saiedian, 2021).

Este caso é um dos casos que representam como a arquitetura da ciberdemocracia pode ser "hackeada" para fins antidemocráticos, com o uso de perfilamento psicográfico para disseminar desinformação, manipular o eleitorado e corroer a integridade do processo eleitoral (Costa, 2024). Nesse sentido, ao utilizar dados para criar perfis psicográficos, como no caso da CA, o objetivo transcende o monitoramento para ativamente moldar o comportamento e o resultado de processos eleitorais. Isso corrompe a essência da ciberdemocracia e substitui o debate público informado pela modulação comportamental oculta.

9. A retórica da vigilância: discurso legislativo e justificativas

No Brasil, Ranieri e Tavares (2020) abordam as tentativas de normalização da utilização de câmeras em ambientes escolares brasileiros na justificativa principal da garantia da segurança. Na visão das autoras, a questão da privacidade tem enfoque no alerta à necessidade de legislações e regulações para que se controle a circulação e o uso das imagens provenientes desses sistemas, deslocando-se da alegação de violação da intimidade.

Embora o Brasil possua a Lei Geral de Proteção de Dados (LGPD), ela não abrange o tratamento de dados pessoais para fins de segurança pública, e mesmo com as controvérsias éticas, projetos de lei como 391/2019 em Minas Gerais e 318/2019 no Rio de Janeiro visam à utilização de sistemas de reconhecimento facial em espaços públicos, mesmo com a ausência de uma legislação que garanta a proteção da privacidade dos dados da população (Cavalcanti, 2022).

Por outro lado, no contexto global, Vagianos e Stavrou (2023) apontam para os riscos dos sistemas de vigilância de Inteligência Artificial (IA) para a democracia e os direitos humanos na China. Esses sistemas possibilitam a coleta e manipulação massiva de dados pessoais, utilizados para espalhar desinformação e restringir as liberdades individuais da população.

Além disso, tais sistemas refletem vieses discriminatórios e são instrumentalizados para o controle político e repressão de minorias, como exemplo, os sistemas de reconhecimento facial na China intensificam a perseguição de minorias étnicas, como os uigures.

Woods (2025) ainda define os sistemas de vigilância chineses como uma relação de parceria entre empresas privadas e o Estado, na qual as empresas são participantes ativas desse processo, com o governo chinês aproveitando-se das capacidades tecnológicas das empresas privadas.

Adicionalmente, para Farinella (2023), legislações recentes na China, como a Personal Information Protection Law (PIPL) e a Data Security Law (DSL), demonstram maior preocupação em assegurar o controle estatal e soberano dos dados do que em proteger a privacidade individual dos cidadãos. Durante a pandemia de COVID-19, o governo utilizou a crise sanitária como justificativa para ampliar e normatizar os mecanismos de vigilância (FARINELLA, 2023; VAGIANOS; STAVROU, 2023).

Nos Estados Unidos, a dificuldade em alcançar consenso político sobre os limites da vigilância decorre, em grande parte, da incerteza e das ambiguidades morais que permeiam o tema. Conforme analisam Almeida, Shmarko e Lomas (2021), o cenário legislativo norte-americano é fragmentado pela ausência de uma lei federal de proteção de dados, o que faz com que a responsabilização pelo uso indevido de sistemas de reconhecimento facial dependa de ações judiciais individuais — geralmente lentas e ineficazes.

Os autores ainda destacam que a utilização desses sistemas é frequentemente justificada pelas autoridades policiais sob o argumento de garantir a segurança pública, apesar das controvérsias éticas. Essa prática tem sido questionada até mesmo por

grandes empresas de tecnologia, algumas das quais declararam que suspenderiam a venda dessas ferramentas ao governo caso não houvesse regulamentação adequada.

No âmbito legislativo internacional, destaca-se a entrada em vigor, em 2024, do Regulamento de Inteligência Artificial da União Europeia, que estabelece parâmetros de regulação da tecnologia. De forma similar, no Brasil tramita o Projeto de Lei nº 2338/2023 (BRASIL, Senado Federal, 2023), que busca disciplinar o uso da inteligência artificial, mas ainda apresenta lacunas e preocupa especialistas quanto à sua sobreposição com a Lei Geral de Proteção de Dados (LGPD) (Vitorino; Fraga; Alexandre, 2024).

O que emerge desses exemplos é um processo consistente de normalização da vigilância por meio de discursos que encontram, na esfera legislativa, seu principal campo de legitimação. Iniciativas como o Regulamento europeu de IA e o PL 2338/2023 representam tentativas de impor limites, mas enfrentam a força retórica que naturaliza a vigilância como condição necessária de segurança e eficiência social.

10. Metodologia

A pesquisa adota uma abordagem qualitativa, crítica, documental e comparativa, orientada pela análise do discurso e pela interpretação político-normativa das tecnologias de vigilância em massa. O delineamento metodológico foi estruturado em três etapas complementares, organizadas de modo a possibilitar a identificação dos mecanismos de legitimação legislativa da vigilância, a análise crítica das tecnologias envolvidas e a comparação entre distintos modelos normativos no cenário internacional.

A primeira etapa consistiu no mapeamento e na análise dos discursos e estratégias retóricas mobilizados em ambientes legislativos para justificar a adoção de tecnologias de vigilância em massa.

Para tanto, realizou-se um levantamento bibliográfico e documental de materiais produzidos entre 2020 e 2025, referentes ao Brasil, aos Estados Unidos e à China, países selecionados por representarem modelos políticos, institucionais e regulatórios distintos. O corpus documental incluiu projetos de lei, regulamentos, marcos normativos, relatórios institucionais e produções científicas, examinados a partir da

identificação de justificativas recorrentes, como segurança pública, eficiência administrativa, estabilidade social e combate ao crime.

A segunda etapa teve como objetivo identificar as principais tecnologias contemporâneas de vigilância em massa e os riscos associados à sua implementação. Nessa fase, foi realizado um levantamento de produções científicas, relatórios técnicos e reportagens especializadas publicadas no mesmo período, com ênfase na descrição do funcionamento técnico desses sistemas, nos mecanismos de coleta e processamento de dados e em seus impactos sociais, políticos e democráticos. Essa etapa permitiu relacionar a dimensão normativa da vigilância com sua materialidade tecnológica, evidenciando como determinadas inovações ampliam a capacidade de monitoramento e intensificam assimetrias de poder.

A terceira etapa consistiu em um estudo comparativo entre modelos legislativos democráticos e autoritários, buscando identificar semelhanças e diferenças nas formas de legitimação jurídica da vigilância tecnológica e avaliar os efeitos dessas normativas sobre a prática democrática, a proteção da privacidade e o exercício das liberdades públicas. A comparação foi conduzida de forma sistemática, considerando o contexto político-institucional de cada país e a relação entre Estado, mercado e sociedade civil na governança da vigilância.

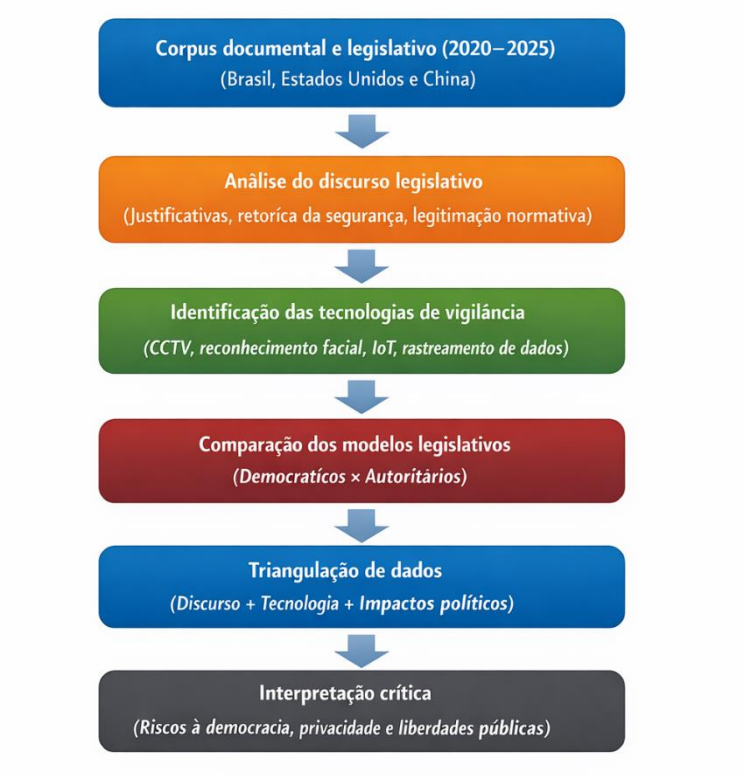
As três etapas foram integradas por meio da triangulação de dados, articulando os resultados da análise discursiva, da identificação tecnológica e da observação dos impactos políticos. Como referencial interpretativo, mobilizaram-se conceitos teóricos clássicos e contemporâneos, como o panoptismo e o biopoder em Foucault, bem como princípios associados à ciberdemocracia, permitindo compreender de que modo a retórica legislativa contribui para a naturalização e aceitação social da vigilância em massa.

Para assegurar rigor metodológico, transparência e replicabilidade, os documentos legislativos analisados foram selecionados a partir dos seguintes critérios: (i) pertinência direta à regulação da vigilância tecnológica ou da inteligência artificial; (ii) tramitação ou vigência no período entre 2020 e 2025; e (iii) incidência sobre espaços públicos, segurança pública ou governança de dados.

Foram excluídos documentos de caráter meramente administrativo ou sem impacto normativo direto. A análise comparativa seguiu um protocolo comum, observando-se: justificativas oficiais, escopo regulatório, atores envolvidos e implicações para os direitos fundamentais, possibilitando contrastar modelos democráticos e autoritários de legitimação da vigilância.

Conforme sintetizado no fluxograma apresentado na Ilustração 1, a pesquisa estrutura-se em um percurso metodológico sequencial e integrado, que parte da análise do discurso legislativo, avança para a identificação das tecnologias de vigilância em massa e culmina na comparação entre modelos normativos democráticos e autoritários. A triangulação dessas etapas permite articular retórica política, infraestrutura tecnológica e impactos sociais, oferecendo uma interpretação crítica dos limites éticos, jurídicos e democráticos da vigilância estatal em sociedades digitais.

Ilustração 1 - Fluxograma das etapas metodológicas



Fonte: Elaborado pelos autores, 2025

11. Modelos legislativos comparados: Brasil, EUA e China

A análise comparativa dos modelos legislativos do Brasil, Estados Unidos e China revela três abordagens distintas para a governança da vigilância em massa, cada qual

refletindo seu respectivo contexto político, cultural e econômico. Embora as justificativas retóricas frequentemente convirjam para a narrativa da segurança, as estruturas legais, os atores dominantes e as consequências para os direitos fundamentais são marcadamente diferentes. Esta seção visa a desvelar como regimes democráticos e autoritários legitimam e normalizam o monitoramento populacional.

12. China: a vigilância como projeto de soberania estatal

O modelo chinês constitui um paradigma de vigilância estatal soberana, no qual o aparato tecnológico é explicitamente instrumentalizado para fins de controle social e de preservação da estabilidade política.

Como analisam Aho e Duffield (2020), o Sistema de Crédito Social (SCS) configura-se como uma resposta "proativa", que se apropria da lógica do capitalismo de vigilância não em favor do lucro corporativo, mas em função da arte de governar (state-craft). Nesse contexto, legislações como a Personal Information Protection Law (PIPL) e a Data Security Law (DSL), embora empreguem uma retórica de proteção, na prática reforçam o monopólio estatal sobre o fluxo informacional, subordinando a privacidade individual às exigências de segurança nacional e de manutenção do regime (MARTINELLI, 2024).

A relação entre o Estado e as grandes empresas de tecnologia na China é simbiótica e estratégica: o governo mobiliza a infraestrutura e a expertise privada para expandir sua capacidade de monitoramento, enquanto as corporações são recompensadas com contratos estatais e a proteção de um mercado interno altamente regulado. A legitimação desse controle em larga escala é sustentada por um discurso oficial de "segurança e harmonia social", que encontra ressonância em setores da população dispostos a valorizar a ordem em detrimento das liberdades individuais (CHEN; ZHAN, 2025).

Entretanto, a consequência mais graves desse arranjo é a instrumentalização política da arquitetura de vigilância para a repressão de minorias. A securitização da etnia uigur, como apontam Baker-Beall e Clark ilustram como tecnologias originalmente justificadas sob o argumento da segurança pública são empregadas como ferramentas de discriminação, controle étnico e silenciamento de dissidências.

13. Estados Unidos: o capitalismo de vigilância e a fragmentação regulatória

Em nítido contraste, o modelo norte-americano materializa o capitalismo de vigilância em um vácuo regulatório. O poder primário de coleta de dados reside nas mãos de um oligopólio de big techs, cuja lógica de acumulação foi teorizada por Zuboff. O Estado, em vez de atuar como principal arquiteto da vigilância, posiciona-se frequentemente como um "cliente" privilegiado dessas tecnologias, especialmente após o 11 de Setembro (SILVA, 2019). A retórica da "guerra ao terror" e da "segurança nacional" serviu como justificativa para expandir o poder de agências como a NSA, que operam em estreita colaboração com empresas de tecnologia, muitas vezes à margem do escrutínio público, conforme revelado por Snowden.

O cenário legislativo é descrito como um "mosaico" ou uma "colcha de retalhos" (ALMEIDA; SHMARKO; LOMAS, 2021). A ausência de uma legislação federal abrangente de proteção de dados, similar à LGPD brasileira ou ao GDPR europeu, cria um ambiente de fragmentação. A responsabilização por abusos depende majoritariamente de ações judiciais individuais, que são lentas e insuficientes para conter o poder estrutural das corporações (SILVA, 2019). A consequência social é a normalização de uma vigilância primariamente comercial que, no entanto, pode ser rapidamente convertida para fins de controle estatal, erodindo a privacidade e a autonomia sem um debate democrático robusto sobre seus limites.

14. Brasil: o modelo híbrido em disputa

O Brasil emerge como um modelo híbrido e em permanente disputa, posicionado entre a tradição europeia de proteção de direitos e as pressões de um discurso securitário crescente. A promulgação da Lei Geral de Proteção de Dados (LGPD), a Lei no 13.709/2018, representou um avanço civilizatório, estabelecendo um arcabouço de direitos e deveres inspirado no GDPR (MARTINELLI, 2024). No entanto, a própria LGPD contém uma exceção crucial: sua não aplicabilidade para fins de segurança pública e persecução penal.

É precisamente nessa brecha que a retórica da vigilância ganha força. Projetos de lei que visam implementar tecnologias de reconhecimento facial em espaços públicos, por exemplo, são frequentemente justificados pela necessidade de combate

ao crime, como apontam Fontes e Lütge (2022). Essa "era de complexa ambiguidade" se manifesta na tensão entre um marco legal que garante a privacidade e uma prática política que busca expandir o monitoramento estatal sem uma regulação específica e adequada para esses fins. A parceria público-privada aqui se dá na contratação de tecnologias de vigilância por órgãos de segurança, muitas vezes com pouca transparência sobre a eficácia e os riscos de vieses discriminatórios. O resultado é um cenário de insegurança jurídica, onde a proteção da privacidade se torna um campo de batalha político e judicial.

O Quadro 1 apresenta a comparação entre China, EUA e Brasil, evidenciando como contextos políticos, legais e econômicos distintos moldam as práticas de monitoramento, parcerias público-privadas e proteção da privacidade em cada país.

Quadro 1 – Modelos legislativos de vigilância

Critério	China	EUA	Brasil
Lógica Dominante	Controle estatal e estabilidade do regime (AHO; DUFFIELD, 2020).	Lucro via extração de dados, com apoio estatal (ZUBOFF, 2021).	Disputa entre direitos (LGPD) e vigilância securitária (MARTINELLI, 2024).
Justificativa	"Segurança nacional" e controle social (BAKER-BEALL; CLARK, 2021).	Antiterrorismo e lógica de mercado (SILVA, 2019).	Segurança pública e combate ao crime (FONTES; LÜTGE, 2022).
Arcabouço Legal	PIPL e DSL priorizam o Estado (AHO; DUFFIELD, 2020).	Sem lei federal geral; regulação fragmentada (ALMEIDA; SHMARKO; LOMAS, 2021).	LGPD com exceções para segurança, gerando brechas.
Parceria Público-Privada	Integração entre Partido e big techs.	Corporações repassam dados ao governo.	Contratação de tecnologias sem transparência.
Consequências	Repressão política e panóptico digital.	Erosão da privacidade e manipulação (ZUBOFF, 2021).	Insegurança jurídica e normalização da vigilância.

Fonte: Elaborada pelos autores, 2025.

Considerações Finais

A pesquisa demonstrou que a retórica da segurança, reiteradamente mobilizada no discurso legislativo, constitui o principal mecanismo contemporâneo de legitimação da vigilância em massa, configurando-se como um risco estrutural às democracias. Ao naturalizar práticas de monitoramento extensivo sob argumentos de proteção coletiva, eficiência administrativa ou estabilidade social, o poder público tende a deslocar o

debate dos direitos fundamentais para uma lógica de exceção permanente, na qual a vigilância se apresenta como condição necessária de governabilidade.

Ao articular os referenciais teóricos de Michel Foucault e Shoshana Zuboff com a análise comparativa dos modelos legislativos da China, dos Estados Unidos e do Brasil, verificou-se que, apesar das diferenças político-institucionais e dos distintos arranjos normativos, a normalização do controle social opera de forma convergente. Em todos os casos, observa-se a subordinação sistemática do direito fundamental à privacidade a supostos bens superiores, como a segurança nacional, a ordem pública ou a eficiência do Estado, o que evidencia a transversalidade do fenômeno da vigilância em massa em regimes democráticos e autoritários.

A análise das tecnologias de vigilância e das narrativas que sustentam sua adoção revelou que a ausência ou a fragilidade de marcos regulatórios específicos, aliada à insuficiência de mecanismos efetivos de accountability, converte a inovação tecnológica em vetor de poder assimétrico. Nesse contexto, a vigilância deixa de ser um instrumento excepcional e passa a integrar de forma estrutural as práticas de governo, corroendo progressivamente os pilares do Estado de Direito e enfraquecendo os controles democráticos sobre o exercício do poder.

Diante desse cenário, a consolidação de um panóptico digital, seja sob a forma de vigilância estatal direta, seja sob a lógica corporativa do capitalismo de vigilância, compromete a promessa emancipatória da ciberdemocracia. Em vez de ampliar a participação cidadã e o pluralismo, a mediação tecnológica passa a operar como mecanismo de modulação comportamental, disciplinamento social e redução do espaço público de deliberação crítica.

Conclui-se, portanto, que o dilema entre segurança e liberdade permanece como um dos desafios centrais da era digital. O futuro das democracias dependerá da capacidade de formular marcos regulatórios transparentes, éticos e efetivos, capazes de submeter a vigilância tecnológica ao escrutínio público, fortalecer a proteção dos direitos fundamentais e assegurar que a defesa da coletividade não se realize à custa da erosão das liberdades individuais.

Referências

AHO, B.; DUFFIELD, R. **Beyond surveillance capitalism: privacy, regulation and big data in Europe and China**. Economy and Society, v. 49, n. 2, p. 187–212, 2020. DOI: https://doi.org/10.1080/03085147.2019.1690275.

ALMEIDA, D.; SHMARKO, K.; LOMAS, E. **The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks**. AI and Ethics, v. 2, n. 3, p. 377–387, 2021. DOI: https://doi.org/10.1007/s43681-021-00077-w.

BAKER-BEALL, C.; CLARK, R. **A post-Copenhagen analysis of China's securitization of the Uyghur: a counterproductive securitization**? Democracy and Security, v. 17, n. 4, p. 427–454, 2021. DOI: https://doi.org/10.1080/17419166.2021.2020037.

BENTHAM, J. **O panóptico**. Tradução de Tomaz Tadeu. 2. ed. Belo Horizonte: Autêntica, 2013.

BRASIL. Senado Federal. **Projeto de Lei nº 2.338**, de 2023. Dispõe sobre o uso da inteligência artificial. Brasília, DF, 2023. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 16 abr. 2025.

CAVALCANTI, L. S. **The role of surveillance technologies in Brazil's public security**: addressing legal and ethical concerns. Padova: Università degli Studi di Padova, 2022.

CHEN, D.; ZHAN, J. V. **When does surveillance trigger resistance?** Public response to escalating digital control in China. Journal of Chinese Political Science, 2025. DOI: https://doi.org/10.1007/s11366-025-09918-5.

COSTA, A. C. M. T. **Vigilância e manipulação digitais: a democracia sob ataque**. 2024. 114 f. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica de Minas Gerais, Belo Horizonte, 2024.

DAVIES, H.; ABRAHAM, Y. **Microsoft launches inquiry into claims Israel used its tech for mass surveillance of Palestinians.** The Guardian, 2025. Disponível em: https://www.theguardian.com/world/2025/aug/15/microsoft-launches-inquiry-claims-israel-used-tech-mass-surveillance-palestinians. Acesso em: 2025.

FARINELLA, N. **Acceptance or resignation?** Surveillance technologies in China between the Social Credit System and Covid-19. Padova: Università degli Studi di Padova, 2023.

FONTES, A. C.; LÜTGE, C. **Vigilância e relações de poder**: o uso de tecnologias de reconhecimento facial e identificação biométrica a distância em espaço público e impactos na vida pública. Direito Público, v. 18, n. 100, 2022. DOI: https://doi.org/10.11117/rdp.v18i100.6203.

FOUCAULT, M. **Vigiar e punir**: nascimento da prisão. Petrópolis: Vozes, 1977.

FOUCAULT, M.; BRANDÃO, E. **Segurança, território, população: curso dado no Collège de France (1977–1978)**. São Paulo: Martins Fontes, 2008.

GANDY, O. H. T**he surveillance society: information technology and bureaucratic social control**. Journal of Communication, v. 39, n. 3, p. 61–76, 1989. DOI: https://doi.org/10.1111/j.1460-2466.1989.tb01040.x.

HUMAN RIGHTS WATCH. **China's algorithms of repression**. 2023. Disponível em: https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass. Acesso em: 2025.

IBM. **What is the Internet of Things (IoT)? 2023**. Disponível em: https://www.ibm.com/think/topics/internet-of-things. Acesso em: 2025.

LEMIEUX, F. **Intelligence and surveillance technologies**. In: _____. Surveillance and intelligence. [S.l.]: Emerald, 2018. p. 165–190. DOI: https://doi.org/10.1108/978-1-78769-171-120181008.

MARTINELLI, C. R. **Capitalismo de vigilância: uma análise do direito fundamental à privacidade na sociedade de controle**. 2024. 97 f. Dissertação (Mestrado em Direitos e Garantias Fundamentais) – Faculdade de Direito de Vitória, Vitória, 2024.

NETO, L. F. et al. Biopolítica em Foucault. Florianópolis: UFSC, 2007.

NURHOPIPAH, A.; HARJOKO, A. **Motion detection and face recognition for CCTV surveillance system**. Indonesian Journal of Computing and Cybernetics Systems, v. 12, n. 2, p. 107–116, 2018. DOI: https://doi.org/10.22146/ijccs.18198.

POMPEU, B.; TRINDADE, E.; SATO, S. K. **Consumo, cidadania e vigilância: reflexões sobre a expansão tecnológica e seus impactos no contexto brasileiro**. Estudos Avançados, v. 38, n. 110, p. 87–104, 2024.

RANIERI, N. B. S.; TAVARES, L. A. **Temas contemporâneos de direito à educação: a utilização de sistema de vigilância por câmeras nas escolas e o direito à privacidade**. Cadernos Jurídicos da Escola Paulista da Magistratura, v. 21, p. 139–149, 2020.

SIERRA, V. M.; FREIRE, S. D. M. **A moderna construção da vigilância e do controle social no Brasil**. Revista Katálysis, v. 24, n. 1, p. 168–176, 2021. DOI: https://doi.org/10.1590/1982-0259.2021.e75233.

SILVA, A. M. **Vigilância estatal em massa no século XXI: conflito de pretensões entre o individual e o coletivo no mundo internacionalizado**. 2019. 153 f. Dissertação (Mestrado em Direito Internacional) – Universidade Católica de Santos, Santos, 2019.

SLOBOGIN, C.; BRAYNE, S. **Surveillance technologies and constitutional law**. Annual Review of Criminology, v. 6, n. 1, p. 219–240, 2022. DOI: https://doi.org/10.1146/annurev-criminol-030421-035102.

STATISTA. **Number of IoT connected devices 2020–2034**, by region. 2025. Disponível em: https://www.statista.com/statistics/1194677/iot-connected-devices-regionally/. Acesso em: 2025.

STEWART, D. R. **Social media and the law**: a guidebook for communication students and professionals. [S.l.]: Routledge, 2012.

THOMPSON, S. A.; WARZEL, C. **Twelve million phones, one dataset, zero privacy**. In: Ethics of data and analytics. [S.l.]: Auerbach Publications, 2022. p. 161–169.

UNDERWOOD, B.; SAIEDIAN, H. **Mass surveillance: a study of past practices and technologies to predict future directions**. Security and Privacy, v. 4, n. 2, 2021. DOI: https://doi.org/10.1002/spy2.142.

VAGIANOS, D.; STAVROU, G. **Surveillance infrastructure and artificial intelligence challenging democracy and human rights in China**. [Revista], v. 20, p. 27, 2023.

VITORINO, B. M.; FRAGA, M. A. O.; ALEXANDRE, W. N. **Evolução da inteligência artificial no legislativo brasileiro**: breve análise do Projeto de Lei nº 2338/2023. In: Anais do 10º Fórum Rondoniense de Pesquisa. Porto Velho, 2024.

WOODS, D. **AI as a tool for surveillance**: China's concave trilemma. Journal of Chinese Political Science, 2025. DOI: https://doi.org/10.1007/s11366-025-09907-8.

ZUBOFF, S. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2021.