A ASCENSÃO DAS BIG TECHS: DESAFIOS E IMPLICAÇÕES PARA A CIBERSEGURANÇA GLOBAL E A NOVA ERA DA SOBERANIA DIGITAL.

THE RISE OF BIG TECH: CHALLENGES AND IMPLICATIONS FOR GLOBAL CYBERSECURITY AND THE NEW ERA OF DIGITAL SOVEREIGNTY

Julia Jacobina de Oliveira[1]

"O pensamento é nuvem
O movimento é drone
O monge no convento
Aguarda o advento de Deus pelo iphone"
(Gilberto Gil)

Resumo: O presente artigo tem por objetivo discorrer sobre a ascensão das Big Techs, seu poder e influência na infraestrutura digital, e suas intersecções com as esferas política e social. Partindo dos conceitos de capitalismo tecnológico contemporâneo, plataformização, tecnofeudalismo e capitalismo de vigilância, o artigo propõe contextualizar o fenômeno das Big Techs como *players* no cenário global e desdobrar os impactos de sua atuação sob a perspectiva da cibersegurança e o uso de dados em massa. Ademais, buscou-se explicar o papel dessas empresas na moldagem de ecossistemas digitais e na sua capacidade de intervir em políticas governamentais.

Palavras-chave: Big Techs; Dados; Capitalismo; Cibersegurança; Tecnologia.

Abstract: This article aims to discuss the rise of Big Tech, its power and influence on digital infrastructure, and its intersections with the political and social spheres. Drawing on the concepts of contemporary technological capitalism, platformisation, technofeudalism, and surveillance capitalism, the article proposes to contextualise the Big Tech phenomenon as players on the global stage and to unfold the impacts of their actions from the perspective of cybersecurity and the use of mass data. Furthermore, it seeks to explain the role of these companies in shaping digital ecosystems and their ability to intervene in governmental policies.

Key-Words: Big Tech; Data; Capitalism; Cybersecurity; Technology.

1 INTRODUÇÃO

Desde o advento da criação do primeiro protótipo da Internet — a ARPANET — e de acontecimentos como a Guerra Fria, o mundo tem experimentado uma evolução constante da tecnologia em suas variadas formas. Em seu livro "BIG TECH, a ascensão dos dados e a morte da política" (2018), o autor Evgeny Morozov até mesmo menciona a afirmação clichê feita por muitos pesquisadores ao dizer que os dados são o petróleo do século XXI. De fato, a sociedade contemporânea é majoritariamente moldada e influenciada por artefatos tecnológicos e essa afirmação se torna ainda mais perceptível

[1] Graduanda em Relações Internacionais pela FMU/SP, com interesse em segurança internacional e cibersegurança. Secretária-geral do Conselho Institucional dos Estudantes de Relações Internacionais (CIERI) da FMU e gerente operacional de comércio exterior.

quando pesquisas indicam que cerca de 68,7% da população mundial navega pela infinitude da Internet.

A ampla adoção da tecnologia em nosso dia a dia, intensificada também pelo capitalismo intrínseco à nossa sociedade, faz surgir uma preocupação global com um tema que transita do espaço físico para o ciberespaço: a segurança. Governos, organizações e indivíduos se tornaram dependentes de soluções de segurança digital ofertadas, majoritariamente, por empresas privadas, criando o que se deu o nome de "complexo industrial da segurança cibernética", por Deibert e Rohozinski (2010). Essa complexidade e os efeitos do *crowdsourcing* evidenciam como a dependência em relação aos novos modos de fluxo informacional dá um enorme poder de controle sobre nós àqueles em posição de controlá-los (CASTELLS, 1996).

Nesse contexto, as Big Techs desempenham um papel tanto central quanto ambíguo, com seu imenso poder financeiro e controle sobre a infraestrutura digital. Empresas como Amazon, Apple, Meta e Microsoft atualmente vão além de meros atores corporativos, elas se estabelecem como verdadeiros players do cenário internacional, detendo um poder tecnocrático que as legitimam como atores tão importantes e as tornam capazes de moldar um ambiente político, regulatório e sociocultural favorável à sua expansão e sua influência. Atualmente, é comum se referir a essas grandes corporações como semiautônomas e semissoberanas conforme mencionado por Deibert e Rohozinski (2010), isso porque, Estados soberanos também estão começando a tratar as Big Tech como atores soberanos, de maneira que diplomatas são contratados para trabalhar exclusivamente com o Vale do Silício. É através dessa perspectiva que a pesquisa busca elucidar, em um primeiro momento, como se deu a ascensão das Big Techs e como elas se portam no cenário cibernético, com suas atuais intersecções na esfera política e social. Posteriormente, será realizada uma análise em torno dos riscos da atuação dessas empresas sob o viés da cibersegurança, buscando explicar de que forma são utilizados os dados que permeiam o ciberespaço e de que maneira podem ser usados em decisões estatais e políticas governamentais.

2 METODOLOGIA

A presente pesquisa adota caráter explicativo, buscando, por meio de conceitos e pesquisas já existentes, clarificar o fenômeno da ascensão das Big Techs. Não obstante, o estudo também assume caráter exploratório, buscando um aprofundamento na questão das infraestruturas digitais globais e nas intersecções entre as Big Techs e as esferas política e social, explorando os riscos da atuação dessas corporações sob a ótica da

cibersegurança. O delineamento do artigo será predominantemente bibliográfico e documental, articulado por meio de literatura especializada, artigos científicos, relatórios e outros periódicos relevantes. Ademais, a perspectiva de tratamento dos dados seguirá uma abordagem qualitativa, priorizando a análise de documentos disponíveis.

3 FENÔMENO DE ASCENSÃO DAS BIG TECHS

O surgimento e a ascensão das Big Techs estão intrinsecamente ligados à atual revolução tecnológica que se expande exponencialmente em razão de sua capacidade de criar uma interface entre campos tecnológicos (CASTELLS, 1996). Empresas como a Microsoft, fundada em 1975, e a Google, em 1998, são exemplos relevantes de como essas organizações se tornaram grandes atores mundiais, incorporando e ampliando suas esferas de atuação. Ademais, a chamada "quarta revolução industrial" com a integração de aparatos tecnológicos e o surgimento da inteligência artificial contribuíram significativamente para o desenvolvimento e consolidação dessas empresas na perspectiva internacional.

Este cenário tem sido denominado por alguns pesquisadores como "capitalismo tecnológico contemporâneo", resultado de um processo entre a revolução tecnológica e o sistema neoliberal global, onde o avanço científico e a lógica econômica capitalista se reforçam mutuamente para sustentar um novo paradigma de poder corporativo. Nesse contexto, as empresas operam sob as estruturas do capitalismo vigente, mas utilizam de sua economia de plataforma para criar e expandir mercados, conquistando públicos diversos que as consolidam cada vez mais em um mundo globalizado de comunicação estreita. Evgeny (2018) descreve esse novo conceito como:

> - Em vez do modelo convencional desgastado, com empresas privadas competindo por consumidores, estamos testemunhando o surgimento de um novo modelo, aparentemente mais nivelado e participativo, no qual os consumidores interagem diretamente uns com os outros. Com um celular no bolso, de repente os indivíduos podem realizar coisas que antes só eram possíveis por intermédio de um conjunto de instituições. (MOROZOV, 2018, p. 55)

Ainda, é notória a utilização, pelas Big Techs, da coleta e análise de quantidades expressivas de dados, caracterizados como *Big Data*[2], que permitem a criação de serviços

[2] Big Data refere-se a coleções extremamente grandes e diversas de dados estruturados, não estruturados e semiestruturados que continuam a crescer exponencialmente com o tempo. GOOGLE CLOUD. O que

personalizados para atender cada indivíduo e suas supostas necessidades, tendo como resultado um ecossistema digital marcado por um ciclo autoperpetuante de benefícios crescentes para as Big Techs, conforme apontado por Khanal et al. (2024).

É sob esse ponto de vista que essas corporações são criadas majoritariamente em países desenvolvidos que buscam constantemente instaurar suas políticas e ideais em Estados em desenvolvimento conforme analisado pelo Instituto Tricontinental de Pesquisa Social (2021). Estes, por sua vez, frequentemente aderem a essas empresas como um fator crucial de evolução tecnológica. A influência dessas corporações em nações em desenvolvimento é um reflexo do crescimento desenfreado que as Big Techs adquiriram em escala global, uma vez que as maiores Big Techs atuais, tal como Apple, Google, Amazon, META e X (antigo Twitter), concentram um valor de mercado agregado superior a 10 trilhões de dólares, valor esse que ultrapassa até mesmo o PIB somado da América Latina, e revela o grande poder monopolista que as grandes empresas possuem e a evidente concentração de capital que caracteriza o capitalismo dadocêntrico e as indústrias de *TIC*[3].

Atualmente, como mencionado por Morozov (2018), tudo é mediado pela tecnologia, tudo o que fazemos pode ser monetizado, aperfeiçoado e integrado em um perfil. Essa onipresença tecnológica está intrinsecamente ligada à "plataformização" e à ascensão massiva das Big Techs. Essas corporações não apenas controlam infraestruturas digitais e tecnologias de ponta, mas também estabelecem as normas que regem as interações entre usuários, concorrentes e clientes. A influência dessas empresas no cotidiano é tão profunda que a dependência de seus serviços por parte de indivíduos e entidades, sejam estatais ou não, é inegável. Exemplos como o uso do aplicativo Uber para locomoção e o uso generalizado de redes sociais para a promoção pessoal demonstram a extensão dessa dependência. Tal cenário evidencia a crescente ascensão dessas empresas, impulsionada pela participação dos usuários, e a consolidação do Vale do Silício como um polo dominante na concepção e direcionamento das tecnologias contemporâneas.

De tal maneira, a ascensão das Big Techs, conforme supramencionado, está diretamente vinculada à revolução tecnológica e à conformação do capitalismo contemporâneo, que as consolidou como atores hegemônicos no cenário global. Essa concentração de influência, que lhes confere a capacidade de controlar e moldar ecossistemas digitais, estabelece a essência para uma análise aprofundada sobre a extensão do domínio dessas Big Techs na própria infraestrutura digital global.

é Big Data?: exemplos e benefícios. [S. l.], [2024]. Disponível em: https://cloud.google.com/learn/what-is-big-data?hl=pt-BR.

[3] Tecnologias da Informação e Comunicação.

3.1 O PODER DAS BIG TECHS E A HEGEMONIA NA INFRAESTRUTURA DIGITAL

O domínio das Big Techs da infraestrutura digital se manifesta em diversas frentes, desde a propriedade e controle de vastas redes de dados até a influência sobre a comunicação e a informação em escala global ao controlar informações em plataformas digitais, como mídias sociais e mecanismos de busca. Por meio das plataformas utilizadas atualmente, elas conseguem gerenciar de maneira seletiva a visibilidade do conteúdo online, o que lhes permite influenciar as questões que recebem atenção tanto do público quanto das próprias empresas. Esse tipo de prioridade seletiva abrange desde o discurso político até narrativas e temas sociais diversos.

Nesse contexto, Campos e Andrade (2023) argumentam que *"a vigilância e a coleta de dados e de informações de caráter pessoal, além de, em muitos casos, ferir direitos humanos e motivar crimes, podem conduzir a um modelo de negócio monopolista, anticoncorrencial"*. Um exemplo comum a ser considerado é o uso de assistentes pessoais como o Google Assistente, nos quais os usuários, em troca de conveniências cotidianas – como o monitoramento de e-mails, a recomendação de restaurantes personalizados ou a verificação das condições de tráfego até a residência –, cedem dados de suas vidas pessoais para a esfera privada.

A percepção de que nossos dados estão protegidos por políticas de privacidade é, contudo, questionada por Morozov (2018), que argumenta que nós estamos sendo "ludibriados" quando nossos dados acabam no balanço dos ativos do Google ou quando os mesmos são utilizados para customizar e estruturar nosso mundo de maneira pouco transparente e pouco desejável. Essa prática se caracteriza, de certo modo, como um meio de dominação através das infraestruturas digitais, conceito que Shoshana Zuboff (2021) nomeia como *capitalismo de vigilância*[4], conforme se observa:

Embora alguns desses dados sejam aplicados para o aprimoramento de produtos e serviços, o restante é declarado como superávit comportamental do proprietário, alimentando avançados processos de fabricação conhecidos como "inteligência de máquina" e manufaturado em produtos de predição que antecipam o que um determinado indivíduo faria agora, daqui a pouco e mais tarde. (ZUBOFF, 2021, p. 22).

De tal maneira, essa presença constante se estende para além do consumidor final e cria um ecossistema de dependência para outras empresas. Os dados são o elemento-chave das Big Techs, e por dominarem esses dados, elas monopolizam o Vale do Silício e

[4] O capitalismo de vigilância reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais.

as estruturas do ciberespaço e, consequentemente, outras empresas são forçadas a recorrer aos seus serviços, sob pena de perderem alcance e relevância no mercado. Um exemplo atual são as editoras de livros que dão preferência a fornecer os livros para a Amazon, se adequando às suas exigências em troca de uma eficácia e rapidez em fazer o livro chegar no público-alvo — através de uma base de dados — sem que o consumidor precise até mesmo sair de sua casa.[5]

Essa infraestrutura, que inclui desde dados, cabos submarinos até tecnologias avançadas como a inteligência artificial e a computação em nuvem, torna-se um ponto de controle estratégico. Esse controle pode ser metaforicamente entendido como um feudalismo contemporâneo, onde as plataformas e a infraestrutura digital atuam como os "feudos" da era moderna, e as Big Techs, como os "senhores feudais" que detêm o controle sobre esses domínios. Usuários e empresas menores, ao dependerem dessas plataformas para operar e interagir, tornam-se, por consequência, "vassalos" que pagam tributos, não com bens ou capital físico, mas com dados e informações. O conceito de tecnofeudalismo, desenvolvido por Yanis Varoufakis (2025), busca explicar então sob um ponto de vista histórico como a sociedade tecnológica funciona.

Não obstante, essa nova forma de poder não se detém às empresas e indivíduos, como será discorrido com detalhes no próximo tópico. As Big Techs utilizam de sua base de dados para se aproximar de governos em escala global e nacional, especialmente daqueles em desenvolvimento, que anseiam por tecnologias como meio de "salvação" e acabam cedendo a participação dessas grandes corporações, tornando-se dependentes de seus serviços e permitindo sua monetização crescente em um ciclo contínuo, conforme pontua Evgeny Morozov (2018, p. 60). Dessa forma, os dados ainda permanecem sob a governança das Big Techs e não dos governos, em uma retórica que mescla vigilância e inovação.

Essa perspectiva da centralização da infraestrutura digital levanta questões críticas sobre a soberania tecnológica e a capacidade de inovação fora dos ecossistemas dominados por essas gigantes, visto que atualmente, é praticamente inviável estar isento da influência dessas grandes corporações, uma vez que a mediação das Big Techs permeia praticamente todos os aspectos de nosso cotidiano.

[5] Como a Amazon dominou vendas de livros no Brasil em apenas 9 anos. Disponível em: <https://www.bbc.com/portuguese/articles/c4nwprveg0wo>.

3.2 INTERSECÇÕES ENTRE AS BIG RTECHS E AS ESFERAS POLÍTICA E SOCIAL

A influência das Big Techs na contemporaneidade vai além de uma perspectiva econômica, transpondo profundamente as esferas política e social. Conforme supramencionado (ver Tópico 2.1), essas grandes corporações estão em praticamente tudo que consumimos no nosso dia a dia. Ao controlarem os algoritmos que determinam o que os usuários veem e ouvem, essas empresas exercem uma influência demasiada sobre as narrativas sociais e políticas, assim, o ciberespaço se torna um palco para a manifestação de seu poder de comunicação e manipulação de informações. Um exemplo a ser utilizado é o caso do vídeo do deputado brasileiro Nikolas Ferreira (PL) sobre o Pix, impulsionado no Instagram com um investimento de R$ 750 mil, onde foi demonstrado que, ainda que de maneira implícita, a plataforma teve sua participação na disseminação de uma desinformação[6]. O fato exemplificado expõe que, conforme mencionado, as Big Techs têm o poder de coibir ou não o que consideram fake news, conforme explicado por Paulo Feldmann (2024) em seu artigo *"O assombroso poder das big techs na economia e na política dos países"*.

O controle de algoritmos confere, então, às grandes corporações a capacidade de intervir e influenciar debates políticos e eleições, impactando diretamente a esfera política por meio da tecnologia. Essa participação ocorre por meio de diversas estratégias, incluindo campanhas de comunicação, posicionamentos em redes sociais, apoio a causas e promoção de discursos que favorecem suas ideologias. Conforme o Dossiê nº 46 do Instituto Tricontinental de Pesquisa Social (2021), a ascensão das Big Techs, enquanto expressão do capitalismo contemporâneo, é acompanhada por uma significativa ofensiva ideológica fundamentada no individualismo, no discurso empreendedor e na negação da política (discurso da neutralidade).[7]

Ademais, a intersecção entre as esferas políticas e sociais com as Big Techs tornou-se uma prática tão comum que essas empresas dedicam recursos jurídicos

para estabelecer, por meio de um lobby, estratégias que visam moldar o âmbito legislativo em favor de seu expansionismo, protegendo seus interesses e evitando restrições que poderiam limitar seu crescimento ou modelo de negócios, como por exemplo o financiamento de campanhas políticas, como o apoio do bilionário Elon Musk à campanha presidencial de Donald Trump em 2024. O exemplo pode ser utilizado para

[6] PAULO MOTORYN. Nikolas gastou R$ 750 mil na Meta para vender cursos. Eu comprei. Disponível em: <https://www.intercept.com.br/2025/07/03/nikolas-meta-curso-destra/>.
[7] DOSSIÊ, N. BIG TECHS E OS DESAFIOS ATUAIS PARA A LUTA DE CLASSES. Disponível em: <https://thetricontinental.org/wp-content/uploads/2021/11/20211026_Dossier-46_PT_Web.pdf>.

explicar como essas corporações projetam sua participação em cargos políticos, ato que permite que elas se beneficiem de conhecimentos internos e exerçam pressão de modo a garantir que suas vozes sejam ouvidas e reconhecidas nos corredores do poder.

Ao se inserirem nos campos políticos e sociais, essas empresas estabelecem colaborações com governos em projetos tecnológicos, apresentando-os como soluções inovadoras para desafios sociais, políticos e ambientais, mas que, na prática, transferem para o setor privado funções que tradicionalmente pertencem ao Estado. Essa participação ativa permite a coleta de dados que outrora fora mencionada, expandindo sistemas de vigilância internacionais e criando uma dependência estatal no poder dessas grandes empresas. De tal maneira, serviços de responsabilidade do Estado, como saúde, transporte e educação, se tornam mercadorias para as empresas que mascaram suas técnicas de dominação através do discurso da eficiência e da "inteligentificação" da vida, conforme mencionado por Evgeny (2018). Esse foco na vida inteligente se manifesta através desses projetos e aumenta a dependência de plataformas privadas para a gestão de informações cruciais.

Essa influência direta que conecta todos esses atores é crucial para as Big Techs, especialmente em um cenário onde a regulação do espaço digital é uma tarefa complexa. Conforme ressaltado por Feldmann (2024), os governos enfrentam dificuldades em controlar esse território imenso que é o ciberespaço, o que garante às Big Techs uma vantagem competitiva significativa, pois elas possuem a competência e a habilidade para atuar nesse ambiente desregulado e o usam a seu favor de uma maneira sutil muitas vezes imperceptível aos olhos da sociedade e até dos legisladores. Essa vantagem se revela na forma como essas corporações coletam e monetizam dados, na maneira como seus algoritmos moldam o comportamento do usuário e na sua capacidade de influenciar narrativas sem a devida transparência e responsabilização. É através desse acesso, que se configura um dos grandes problemas da atualidade, a maneira não somente como as Big Techs estão intrinsecamente presentes nosso dia a dia, nossos governos e os serviços que utilizamos, mas como essa presença onipotente do setor privado, ameaça o que conhecemos por cibersegurança criando vulnerabilidades significativas que tangem não somente a segurança nacional, mas também a segurança internacional.

4 IMPACTOS E RISCOS NA CIBERSEGURANÇA

Em um mundo onde a segurança atingiu um papel constitutivo e uma visibilidade sem precedentes na vida contemporânea (STEVENS, 2015), a hegemonia das Big Techs, consolidada através do domínio da infraestrutura digital e de sua profunda intersecção

com as esferas política e social, cria um novo e complexo paradigma para a cibersegurança global. A centralização massiva de dados e o controle sobre os serviços digitais essenciais transformam essas corporações em pontos de vulnerabilidade, uma vez que a concentração de poder que lhes confere uma capacidade indubitável de inovação também gera, consequentemente, uma superfície de ataque de valor sem precedentes, tornando a segurança tanto uma condição a ser alcançada quanto um processo pelo qual essa condição é atingida no ecossistema digital, conforme mencionado por Tim Stevens (2015).

De maneira tal, um simples vazamento de dados dessas empresas pode desencadear um efeito cascata que afeta não só a vida cotidiana de seus usuários, como também serviços governamentais, como recentemente, onde houve um mega vazamento — considerado o maior da história — de plataformas como Apple, Google, Facebook e de serviços do governo que expôs mais de 16 bilhões de senhas e dados que podiam ser facilmente acessados online e consequentemente culminar em invasões de contas, entre outros crimes cibernéticos.

É notório dizer que as grandes corporações constituem um paradoxo sob a perspectiva de segurança, pois são entidades que propagam seus métodos de securitização cibernética com defesas notáveis em suas infraestruturas e seus investimentos para tal. Contudo, ao mesmo tempo, esse papel de guardiã é contestado, uma vez que sua influência e dominância, combinada com operações internas que não são de conhecimento do público, criam um ambiente onde vulnerabilidades podem não apenas existir, mas também serem exploradas em larga escala por uma gama diversificada de atores, sejam eles estatais ou não. De forma que, ao mesmo tempo em que protegem, essas corporações concentram um poder e uma complexidade que representam um risco inerente para a estabilidade e segurança da sociedade conectada.

Não obstante, os riscos atuais vão além de roubos e/ou vazamento de dados em larga escala do público que se utiliza dessas plataformas comandadas pelas Big Techs. De forma que, as ameaças cibernéticas se tornaram verdadeiras armas políticas de manipulação, espionagem e sabotagem através de ataques de grupos avançados conhecidos como *APTs (ameaças avançadas persistentes)*[8]. Frequentemente financiados por Estados, esses grupos utilizam táticas modernizadas para invadir redes, evitar a detecção e permanecer ativos por longos períodos, com o objetivo de cumprir suas missões, onde o objetivo principal deixa de ser apenas o roubo de dados e passa ser ativamente a contribuir para o interrompimento de projetos, missões ou programas de organizações-

[8] COMO a ciberguerra global vai impactar a segurança no Brasil. Ministério Público do Estado de Mato Grosso, 2022. Disponível em: https://www.mpmt.mp.br/portalcao/news/1217/158392/como-a-ciberguerra-global-vai-impactar-a-seguranca-no-brasil/111.

alvo, transformando a infraestrutura digital em um verdadeiro campo de guerra.

Diversos especialistas já definem as Big Techs como um braço armado de conflitos geopolíticos nesse novo cenário. Por exemplo, o Google Earth pode ser usado para pesquisa geográfica ou para o direcionamento de ataques militares, da mesma maneira que o HoloLens da Microsoft, inicialmente um dispositivo para jogos, agora tem aplicações militares significativas e o reconhecimento facial da Amazon pode ser usado para transações seguras ou para vigilância em massa. A sede de defesa dos Estados Unidos (Pentágono) foi responsável pelo financiamento de inúmeras startups no Vale do Silício o que ressalta o DNA da indústria de defesa presente nas gigantes da tecnologia de hoje e exemplifica a intersecção entre as questões de cibersegurança que permeiam os Estados e as grandes corporações que dominam o cenário mundial. Pode-se dizer que, embora tenhamos absorvido e integrado rapidamente smartphones e tablets em nossas vidas, raramente refletimos sobre como os dados armazenados e transmitidos por esses dispositivos podem facilmente ser militarizados. (NASSIF, 2024)

É sob a perspectiva previamente supracitada que a segurança cibernética e sua relação com as Big Techs sai do campo apenas corporativo e se torna um elemento que passa a compor as Relações Internacionais e o conceito de soberania digital. Como uma arena geopolítica moderna, o ciberespaço se torna alvo até mesmo de forças armadas, como por exemplo, descrito recentemente no Livro Branco da Defesa da China (2019), a busca das forças armadas chinesas em manter protegidas as suas informações e sua soberania cibernética nacional como forma de estabilidade social.

Faz-se necessário pontuar também, que os impactos das Big Techs na cibersegurança vão além das questões geopolíticas e tensões entre Estados. A ideia dessa nova era de soberania digital vem diretamente relacionada com a securitização da vida cotidiana e a segurança como um produto e não mais como um bem social. Conforme descrito por Luiza Lobato (2016), as empresas privadas não apenas contribuem para o desenvolvimento de tecnologias de informação centrais, elas desempenham simultaneamente um papel importante na produção de segurança no domínio virtual, seja desenvolvendo *software* e *hardware*, executando plataformas e redes online ou comercializando produtos e soluções para tornar a experiência online mais "segura". Dessa forma, as pressões para "proteger" o ciberespaço acabaram se tornando uma grande oportunidade de negócios para empresas privadas, que disputam para garantir a melhor segurança, criando uma "mercadização" (LOBATO, 2016) dessa segurança cibernética.

Essa dinâmica de proteção pode levar a uma situação em que os problemas de segurança são apresentados de forma a justificar a necessidade de mais produtos e serviços das próprias Big Techs, consolidando sua posição dominante e limitando a capacidade de

alternativas independentes surgirem. A promessa de uma segurança total mascara muitas das vezes a realidade de um sistema intrinsecamente propenso a falhas, onde a solução é sempre oferecida por quem detém o controle da infraestrutura. Essa estratégia de monopolização, por sua vez, gera uma dependência crescente dos usuários e até mesmo de governos em relação aos serviços e plataformas das grandes corporações, conforme já mencionado na pesquisa. À medida que mais aspectos da vida cotidiana migram para o ambiente digital controlado por essas empresas, a capacidade de operar independentemente ou de buscar soluções alternativas diminui drasticamente, uma vez que a conexão entre diferentes ecossistemas tecnológicos cria barreiras de entrada para novas empresas, fazendo com que os usuários permaneçam em um ciclo de dependência. Em um cenário onde a cibersegurança é cada vez mais vital, a concentração de poder e conhecimento nas mãos de poucas entidades privadas representa um risco sistêmico, pois qualquer falha ou decisão unilateral dessas empresas pode ter consequências catastróficas para a sociedade como um todo,

reforçando a ideia de que, conforme supracitado, a segurança se tornou um produto exclusivo, e não um direito universalmente acessível.

4.1 A GOVERNANÇA DOS DADOS E A VIGILÂNCIA CAPITALISTA

A transição para uma sociedade majoritariamente tecnocrática com a forte presença das Big Techs indubitavelmente redefiniu o que se entende fundamentalmente por poder, vigilância e segurança. Conforme supramencionado na pesquisa, a hegemonia dessas corporações não se pauta somente na dominância infraestrutural, ou seja, não apenas no cerne das plataformas, mas na sua capacidade de extrair e utilizar o que, conforme Evgeny Morozov (2018), é o petróleo do século XXI, os dados. É sob esse viés que convém afirmar que a governança desse arsenal de dados se tornou o principal pilar do capitalismo de vigilância, transformando a experiência humana em matéria-prima e, consequentemente, criando vulnerabilidades tanto para a cibersegurança individual quanto coletiva.

Esse novo paradigma é, em sua base, estruturado sob o conceito de superávit comportamental conforme definido por Shoshana Zuboff (2021), que é “alimentado” através dos dados que são gerados nas plataformas. Convém ressaltar que as referências para esse superávit e arsenal, não está apenas naquilo que clicamos ou em nossas pesquisas, mas sim em um universo de metadados que contabiliza o tempo que passamos em uma imagem, a velocidade com que digitamos, os locais que frequentamos e aqueles que preferimos não ir e até mesmo nossas emoções interpretadas por meio de análises de texto e reconhecimento facial. Ou seja, até mesmo quando não estamos “online”, os nossos

dados estão sendo extraídos e refinados pelas corporações.

De tal maneira, a maior parte das plataformas que permeiam as Big Techs são "gratuitas", o que gera uma falsa sensação no indivíduo de estar usufruindo de uma evolução da sociedade tecnocrática sem precisar desembolsar nada. Verdadeiramente, não precisamos pagar com cédulas ou moedas para acessar essas plataformas, contudo, como as grandes corporações operam sob os vieses do capitalismo, a gratuidade é apenas um disfarce utilizado que mascara o real pagamento que fazemos com os nossos dados, conforme explicado por Evgeny Morozov (2018). Um exemplo a ser citado são os sites que possuem programas de fidelidade, onde não precisamos pagar nada para participar e receber "prêmios" e descontos, contudo, fazemos um cadastro onde informamos nosso CPF, data de nascimento e número de celular, ou seja, gratuitamente nós fornecemos nossos dados para a empresa.

Essas ações inofensivas à primeira vista munem o capitalismo de vigilância, uma vez que as empresas passam, através de nossas informações, a comercializar previsões sobre nossas decisões de consumo, nossos ideais políticos e nossas vulnerabilidades para um mercado de clientes interessados em ter uma parcela de influência em nossas ações coletivas e individuais. Conforme destaca Shoshana Zuboff (2021), nessa era tecnocrática, nós não somos os clientes nem mesmo as mercadorias, em vez disso somos os objetos dos quais as matérias-primas (dados) são extraídas e expropriadas para as fábricas de predição, isto é, somos os meios para os objetivos finais dessas corporações. Não obstante, esse modelo corporativo possui uma infraestrutura de segurança frágil, uma vez que extrai e armazena dados de bilhões de indivíduos, criando o que é conhecido por *"pontos únicos de falha (single points of failure)"*[9] que, com um simples vazamento, podem por consequência ser um atrativo para engenharia social, roubo de identidade ou ataques cibernéticos.

Para manter as engrenagens das plataformas funcionando sem quaisquer atritos, as Big Techs se empenharam em desenvolver mecanismos que garantam a legitimação desses serviços, principalmente através da chamada "Política de Privacidade" mencionada anteriormente (ver tópico 2.1). Esse mecanismo foi apresentado como um documento que visa, em maior instância, informar os usuários sobre como seus dados serão utilizados, mas que funciona, na prática, como um instrumento de consentimento para a vigilância conforme mencionado por Morozov (2018). Esse documento é apresentado para aqueles

[9] Um ponto único de falha é um ambiente onde uma única falha pode resultar na perda simultânea da estrutura da lista de recursos de acoplamento para um fluxo de logs e da cópia do buffer de armazenamento local dos dados no sistema que faz a conexão. Ver IBM. What is a single point of failure (SPOF)?. In: IBM Documentation: z/OS Version 3.1.0. [S. l.], 2024. Disponível em: https://www.ibm.com/docs/en/zos/3.1.0?topic=data-what-is-single-point-failure.

que acessam as mais variadas plataformas através de textos longos com inúmeras páginas, termos complexos e leis, que causam estranheza aos usuários que são levados a concordar com a coleta e o tratamento de seus dados em troca do acesso a serviços "gratuitos". Atualmente, essa prática tem sido apresentada através dos *"cookies"*[10] que o usuário pode aceitar ou negar, mas que interfere na interface dos sites e em sua utilização dependendo da resposta. Leis como a *LGPD (Lei Geral de Proteção de Dados)* no Brasil e a *GDPR (General Data Protection Regulation)* na Europa surgiram como tentativas de equilibrar essa relação entre usuário e provedor, contudo, a balança de poder permanece sendo um desafio moderno e que culmina em discussões em diversas partes do globo.

Essa arquitetura de governança de dados, portanto, gera um risco de cibersegurança imensurável, uma vez que a concentração de arsenais de dados mencionada anteriormente como *"Big Data*" se torna responsável pelo que os atuais especialistas cibernéticos determinam como "superfície de ataque", que segundo a empresa americana de segurança cibernética Fortinet, pode ser descrita como o número de todos os pontos possíveis, ou vetores de ataque, onde um usuário não autorizado pode acessar um sistema e extrair dados. Ou seja, esse amontoado de dados compilados torna essas plataformas alvos primários para cibercriminosos, onde um único vazamento pode ter consequências devastadoras.

Um exemplo a ser considerado foi o vazamento de dados de mais de 13 milhões de pessoas pela SPTrans em dezembro de 2022 no Brasil, informações como nome, data de nascimento, endereço, CPF, RG, telefone, e-mail, login e senhas pessoais foram parar na darkweb (CNN BRASIL, 2023). As informações vazadas são a matéria-prima para uma vasta gama de crimes cibernéticos: roubo de identidade, fraudes financeiras, extorsão e espionagem, sendo a última comum entre Estados. Esses crimes não geram impactos apenas financeiros, mas se tornam um empecilho na confiança da sociedade para com o âmbito digital.

Para o indivíduo, ter seus dados expostos representa uma perda de controle sobre a sua própria identidade digital, onde a segurança pessoal deixa de ser uma questão de práticas individuais, como, por exemplo, ter senhas fortes com vários caracteres, e passa a ser uma questão de infraestrutura das grandes corporações sobre as quais o usuário não tem controle. A promessa de segurança feita por essas empresas, conforme mencionado outrora (ver tópico 3), torna-se contraditória, uma vez que, ao mesmo tempo em que oferecem serviços de proteção contra crimes cibernéticos, a sua própria acumulação de

[10] Um pequeno arquivo que é salvo no computador das pessoas para ajudar a armazenar as preferências e outras informações usadas nas páginas da Web que elas visitam. Ver GOOGLE, Como os cookies são usados pelo Google. Disponível em: https://policies.google.com/technologies/cookies?hl=pt-BR.

dados cria um risco e um cenário ideal para que esses ataques aconteçam.

A governança de dados, portanto, não é apenas uma questão de privacidade do indivíduo que utiliza as plataformas, mas deve ser uma preocupação dos estudos de cibersegurança que se desenvolvem na modernidade, uma vez que a forma como os dados são coletados, processados e protegidos define as fronteiras da segurança digital, estabelecendo o cenário para impactos ainda mais amplos sobre a esfera pública e a soberania dos Estados.

4.2 A INFLUÊNCIA SOBRE A ESFERA PÚBLICA E O DESAFIO A AUTONOMIA INDIVIDUAL

É indubitável que, a tecnologia tem alcançado patamares que outrora permaneciam apenas no campo subjetivo da capacidade humana. Mas não somente isso, os aparatos tecnológicos que compõem nosso dia a dia possuem muito mais influência em nossas ações do que percebemos. Como a informação é uma parte integral de toda atividade humana, todos os processos de nossa existência individual e coletiva são diretamente moldados (embora, com certeza, não determinados) pelo novo meio tecnológico. (CASTELLS, 1996).

Para entender como nossas atividades são meticulosamente moldadas pelas Big Techs, é necessário se apropriar dos termos *"bolhas de filtro"* e *"câmaras de eco"*. O primeiro, proposto pelo ativista norte-americano Eli Pariser, refere-se à personalização do conteúdo online que isola intelectualmente os usuários da internet e diminui a diversidade das informações às quais são expostos (CARDON, 2020, apud PARISER, 2011), ou seja, é o método utilizado pelas corporações para filtrar e nos mostrar somente aquilo que gostamos de acordo com os nossos dados fornecidos através de curtidas e compartilhamentos em redes sociais, por exemplo.

O segundo, por sua vez, de acordo com Cardon (2020), se pauta na formação de comunidades virtuais nas quais as pessoas compartilham e recebem informações focadas em seus interesses e alinhadas às suas crenças, como por exemplo a opção de fazer parte de uma comunidade criada no antigo Twitter e mantida no atual X. É assim que o sistema de recomendação, ao aprender e entender as preferências do indivíduo, cria um feed personalizado que o isola de perspectivas divergentes. Inicialmente, embora pareça ser um aparato pensado para considerar a autonomia de cada ser em escolher ver apenas aquilo que lhe interessa, o resultado dessa influência é uma fragmentação da esfera pública e uma intensificação da polarização política ao mesmo tempo em que a desinformação, nesse contexto, deixa de ser um mero "ruído" e se torna uma arma de ciberataque direcionada ao âmbito social.

O fenômeno da desinformação e da manipulação é intensificado pelos algoritmos das plataformas, que priorizam conteúdos com alto potencial de engajamento (FLOR, 2025). Uma vez que o modelo utilizado é baseado na economia da atenção, priorizando conteúdos que, de acordo com o perfil traçado pelos dados expostos, vão gerar uma reação emocional do usuário que o fará permanecer mais tempo ali e consequentemente dar mais engajamento, conforme mencionado por Katarine Flor (2025).

É dessa maneira que notícias sensacionalistas são divulgadas por toda parte e se espalham com rapidez, comprovado por um estudo realizado pelo Massachusetts Institute of Technology (MIT) que realizou um experimento onde cerca de 126 mil boatos foram espalhados por cerca de 3 milhões de pessoas no antigo Twitter. As notícias falsas alcançaram entre mil e dez mil pessoas, enquanto as notícias verdadeiras ficaram contidas em um grupo de cerca de mil pessoas apenas. Esse ciclo evidencia o ambiente no qual as Big Techs constroem o seu domínio e o aparato da algoritmização como fonte da manipulação de opiniões públicas e ameaça à autonomia individual dentro do ciberespaço.

O documentário "Dilema das Redes", disponível na Netflix e dirigido por Jeff Orlowski, reúne ex-funcionários do primeiro escalão de gigantes da tecnologia, como ex-executivos do Google, do Facebook e do Youtube, para, de uma perspectiva interna, alertar os telespectadores dos artefatos manipuladores que existem por detrás das redes sociais. O documentário é quase um paradoxo, por assim dizer, uma vez que é uma crítica às Big Techs sendo exibida dentro de uma Big Tech. Conforme ressaltado por Tatiana Dias (2020) em sua resenha sobre o documentário para o jornal Intercept Brasil, um dos ex-funcionários exemplificou seu trabalho como o de hackers, onde eles encontraram uma vulnerabilidade no nosso cérebro, que precisa de constante atenção, dopamina e reconhecimento, e tornaram aquela sensação acessível em segundos mexendo no celular e navegando na Internet e dessa forma exploraram a falha, criando maneiras de recompensa instantânea, e construindo ferramentas que aumentassem o nosso tempo online – e, assim, a possibilidade de tornar nossas interações mais lucrativas para os anunciantes. No documentário, é mencionada também a proibição dos ex-funcionários quanto ao acesso de seus filhos nas plataformas que eles mesmos criaram e isso leva a um questionamento de que, se até sob a perspectiva interna das redes, há um processo de influência e manipulação, o que nos falta para tomar uma atitude quanto a isso?

Evgeny Morozov (2018) aprofunda a discussão sobre a influência na esfera pública utilizando como base o conceito de *física social*[11] proposto por Alex Pentland. O termo

[11] A física social é o estudo de como comportamentos individuais e interações sociais em redes influenciam o comportamento de grupos, comunidades e sociedades maiores. Essa abordagem analisa dados de fontes como mídias sociais, dispositivos móveis e padrões de comunicação para revelar os

busca em suma compreender como comportamentos coletivos, como tomada de decisão em grupo, cooperação e inovação, são desencadeados por ações individuais como compartilhamentos, curtidas ou comentários, rastreando como essas pequenas ações aparentemente isoladas contribuem para fenômenos de grande escala, revelando como as informações ou o comportamento — seja presencial ou online — se propagam pela sociedade. (Rose E., 2024).

Morozov (2018) aplica esse conceito para explicar como os sistemas que utilizam esse tipo de física não conhecem apenas os nossos gostos ou traçam apenas nosso perfil, mas sim a rastreabilidade se estende para nossos amigos, relacionamentos diversos e pessoas de nosso convívio. De maneira tal, através do acúmulo de dados, as plataformas tecnológicas utilizam de nossos relacionamentos como forma de governança, traçando um perfil social de cada indivíduo que vai ser usado como forma de influência para apresentar novos aplicativos, novas propagandas através das pessoas certas, conforme descreve Pentland:

É o fluxo de ideias e oportunidades entre as pessoas que impulsiona a sociedade, gerando resultados quantitativos em escalas que variam de pequenos grupos a empresas, cidades e até países inteiros. Não podemos mais nos considerar apenas indivíduos racionais que tomam decisões cuidadosamente ponderadas; precisamos incluir os efeitos dinâmicos das redes sociais que influenciam nossas decisões individuais e impulsionam bolhas econômicas, revoluções políticas e a economia da internet. (PENTLAND, A. 2019)

De tal maneira, a persuasão das Big Techs evidencia que uma empresa privada possui a capacidade de inibir e modelar não somente indivíduos comuns, mas também agentes governamentais e líderes estatais, uma prerrogativa que desafia a soberania dos processos democráticos. Essa governabilidade evidencia que não somente a autonomia dos cidadãos comuns está ameaçada, mas também evidencia um déficit democrático onde o poder de regular a fala está concentrado nas mãos das poucas entidades dominantes do Vale do Silício.

4.3 A NOVA ERA DA SOBERANIA DIGITAL E A DEPENDÊNCIA INFRAESTRUTURAL ESTATAL

Se o conceito de soberania outrora se baseava em conquista territorial, a modernidade tecnocrática ressignificou esse conceito. Hoje, quem domina a tecnologia mais avançada também domina o mundo, conforme destacado por Evgeny Morozov

princípios fundamentais do comportamento humano. Rose E. (2024). Física Social. The Decision Lab. Disponivel Em: https://thedecisionlab.com/reference-guide/psychology/social-physics

(2018). De tal maneira, se a governança tecnológica maior repousa nas mãos das Big Techs, nos convém concluir que a ordem contemporânea tem sido vítima de uma corrosão na soberania estatal, uma vez que atingimos um ponto como sociedade tecnológica que nem mesmo os Estados são capazes, em sua maioria, de frear as grandes corporações e acabam por se submeter a elas, consolidando um novo regime de poder. Esse novo período é descrito por Morozov em seu livro "*A ascensão das Big Techs e a morte da política*" (2018) como a substituição da governança antes democrática pelo termo regulação algorítmica, cujos alicerces se encontram em uma utopia tecnocrática que mascara a transferência de poder e decisão do cidadão para a aliança entre o Estado e a corporação tecnológica.

A inserção tecnológica no círculo estatal sempre esteve presente, contudo, a ascensão das Big Techs como atores políticos deve ser entendida no contexto de uma mudança social que promove a tecnologia como a solução definitiva para os maiores desafios da humanidade (Ulnicane & Aden, 2023; Zuboff, 2019). Esse poder tecnocrático as legitimam, fundamentado na crença de que suas plataformas são indubitavelmente democráticas e na relação simbiótica entre seu modelo de negócio e a lógica neoliberal (Ferrari, 2020). Com essa legitimidade, as Big Techs se tornam super empreendedoras de políticas, elas não apenas influenciam o processo político, elas o redesenham, com sua capacidade de posicionar lobistas, pesquisadores e ex-funcionários em posições-chave, elas redefinem problemas sociais para que suas "soluções" tecnológicas pareçam ser as únicas viáveis, ditando a natureza e o momento das janelas de políticas públicas, conforme proposto por Khanal, Zhang e Taeihagh (2024).

O solucionismo tecnológico se tornou um dos maiores desafios da contemporaneidade. Segundo Morozov (2018), o Vale do Silício nos convenceu de que todos os problemas complexos da sociedade — da saúde pública à evasão fiscal — podem ser resolvidos por meio de aplicativos, sensores e ciclos de retroalimentação. Um exemplo é a migração da infraestrutura crítica para o sistema de *nuvem*[12], no qual nos deparamos com serviços essenciais que antes eram de obrigação puramente estatal, operando em diferentes plataformas sob o pretexto de "eficiência", mas que, se for analisado com minúcia, configura uma transferência de controle sobre os ativos de informação sensíveis de uma sociedade nas mãos das grandes corporações.

Não obstante, Evgeny Morozov (2018) complementa que essa visão do solucionismo seduz governos enfraquecidos, que veem na tecnologia uma saída para crises

[12] A nuvem é um vasto espaço de armazenamento online onde pessoas e empresas guardam seus arquivos e aplicativos, acessível de qualquer lugar com conexão à internet. Ver Microsoft Azure. O que é a nuvem?. Disponível em: https://azure.microsoft.com/pt-br/resources/cloud-computing-dictionary/whatis-the-cloud

fiscais e de legitimidade, sob o pretexto de “modernização cívica” onde o resultado final é a ascensão da regulação algorítmica, um novo tipo de governança que substitui leis e debates políticos por mecanismos de feedback e otimização de dados.

De tal maneira, as Big Tech se tornaram onipresentes e onipotentes no processo político. Sua influência e recursos as tornaram entidades quase semiautônomas e semissoberanas, desfrutando de considerável autoridade global (KHANAL; ZHANG; TAEIHAGH, 2024). Essa presença recorrente expõe a nova era da soberania digital, uma vez que até mesmo Estados e atores do eleitorado passaram a tratar as grandes corporações como atores soberanos. Um exemplo claro dessa inserção significativa é a presença do bilionário Elon Musk, dono do X, como membro pleno e ex-conselheiro sênior da Casa Branca no governo de Donald Trump, ou seja, a presença direta de uma Big Tech no âmbito político e estatal que por fim favorece a criação de um ambiente regulatório favorável à sua expansão, muitas vezes resultando em autogovernança com supervisão estatal mínima (Shaleen Khanal, Hongzhou Zhang, Araz Taeihagh, 2024 apud Luitse & Denkena, 2021).

O resultado dessa intersecção é uma colonização do Estado por dentro, onde aplicativos e sensores se conectam diretamente à infraestrutura pública, privatizando, na prática, a governança, conforme descrito por Evgeny Morozov (2018):

O Vale do Silício não propõe abertamente o fim do Estado; pelo contrário, seu Estado ideal é um Estado obcecado por dados, um parceiro comercial. Seu objetivo real é reprogramar o Estado, tornando-o receptivo à lógica da retroalimentação e eliminando outros meios de fazer política. Exigem "dados abertos" e "interoperabilidade", não por um ideal de transparência, mas para que seus aplicativos e sensores possam se conectar diretamente à infraestrutura estatal, privatizando, na prática, a governança. Quando o Estado já privatizou todos os seus ativos físicos, o próximo passo é privatizar seus dados. (MOROZOV, E., 2018)

Essa colonização é evidenciada com a perda do monopólio estatal sobre a inteligência. Através de uma perspectiva histórica, os governos sempre buscaram observar, compreender, prever e moldar o comportamento humano (COZINHA, K., 2021), contudo, as empresas de tecnologia continuam realizando as mesmas funções nos dias atuais, mas sob o contexto das chamadas “pesquisa de mercado” ou “desenvolvimento de produtos”, que mascaram a verdade de que, de uma maneira modernizada, o Estado não conhece mais sua nação. O conhecimento sobre indivíduos e sociedades está sob as infraestruturas de dados de atores do setor privado e essa crescente lacuna de informações, por consequência, deixa os líderes da segurança nacional cada vez mais dependentes de empresas de tecnologia para conduzir missões essenciais, consolidando o que Deibert e Rohozinski (2010) chamaram de “complexo industrial de segurança cibernética”.

Sob essa dinâmica, as empresas não apenas respondem às demandas do governo, mas, por outro lado, procuram ativamente os Estados para vender produtos e serviços de segurança, muitas vezes alimentando um ciclo de exagero baseado no medo para justificar seus próprios produtos. Essa relação turva as linhas de responsabilidade, tornando difícil saber se uma prática de vigilância responde a um governo ou a um contratante privado. A terceirização, usada por governos para mitigar riscos, acaba gerando arranjos que carecem de transparência e colocam a segurança nacional nas mãos de atores cujos interesses comerciais podem não se alinhar com o interesse público. Algumas dessas empresas chegam a competir com os próprios governos pela "condução das hostilidades" no ciberespaço (Harris, 2014).

Assim, em termos simples, as maiores empresas de tecnologia do mundo acumulam um nível de riqueza, influência e presença internacional que antes eram exclusivos dos Estados. Ao se tornarem dependentes de sua infraestrutura, de sua inteligência e de seus serviços de segurança, os próprios Estados se tornam meros inquilinos em sua própria casa digital, estabelecendo uma nova era da soberania digital ao mesmo tempo que representa um risco à democracia.

5 CONSIDERAÇÕES FINAIS

Ao analisar os tópicos desenvolvidos, é possível compreender, portanto, as nuances envolvidas na ascensão das Big Tech como um fenômeno que transcende a inovação tecnológica e os impactos no nosso dia a dia como indivíduos comuns e também em nossa política e espaço cibernético. Em uma passagem na obra contemporânea "*A Era do Capitalismo de Vigilância*", Shoshana Zuboff (2021) descreve que nós celebramos o mundo conectado por causa das muitas maneiras pelas quais ele enriquece nossas capacidades e perspectivas, mas ele gerou novos grandes territórios de ansiedade, perigo e violência conforme o senso de um futuro previsível se esvai por entre nossos dedos.

Em outras palavras, em um mundo onde a tecnologia é um motor de funcionamento da sociedade, as Big Techs se impõem como engrenagens que mantêm o bom funcionamento desse motor. A era do capitalismo tecnológico contemporâneo, onde a revolução digital e a lógica neoliberal se fundem para criar um novo paradigma de poder, a extração massiva de dados, as economias de plataforma e o chamado "tecnofeudalismo" estabelecem ecossistemas de dependências com uma balança de poder desbalanceada e monopolista que garante a autoperpetuação das grandes corporações em um ciclo de dominância corporativa e controle da infraestrutura digital. Consequentemente, se cria um paradoxo cibernético onde as mesmas entidades que oferecem soluções de proteção são,

em virtude da centralização massiva de dados, os maiores pontos de vulnerabilidade.

Um único vazamento pode ter efeitos catastróficos, e a militarização de tecnologias civis transforma o ciberespaço em um campo de batalha geopolítico, onde a segurança deixa de ser um direito para se tornar um produto comercializado.

Não obstante, a pesquisa aponta para a corrosão da soberania estatal na era digital. Governos, seduzidos pelo "solucionismo tecnológico" e enfraquecidos em sua capacidade de regulação, acabam por transferir o controle de infraestruturas críticas e dados sensíveis para o setor privado. Conforme previsto por Morozov (2018), a consequência final é a morte da política como a conhecemos. O desacordo e o conflito, essenciais à democracia, são vistos como falhas da era analógica a serem eliminadas pela coleta de dados. Como previu o escritor Stanisław Lem, a sociedade não pode desistir do fardo de decidir seu próprio destino, abdicando dessa liberdade em prol de um regulador cibernético.

É diante dos fatos elencados que a conclusão desta pesquisa não se propõe a ser um ponto final, mas um convite à reflexão. A discussão sobre a ascensão e hegemonia das Big Techs nos leva a questionar: que modelos de regulação podem efetivamente proteger os direitos dos cidadãos e a soberania dos Estados sem contestar a inovação? De uma maneira mais profunda, o que significaria para os Estados investirem na construção de uma soberania digital real, retomando o controle sobre suas infraestruturas e dados essenciais? A realidade é que, as respostas a essas perguntas não vêm de uma única fonte ou autor, mas da convergência entre uma governança e sociedade digitalmente letrada, capaz de gerir um futuro tecnológico democrático.

REFERÊNCIAS BIBLIOGRÁFICAS

ARIANA. Big Techs e os desafios atuais para a luta de classes. Disponível em: <https://thetricontinental.org/pt-pt/dossier-46-big-tech/>.

CNN BRASIL. SPTrans diz que foi alvo de ataque cibernético e teve dados cadastrais vazados. [S. l.], 2024. Disponível em: <https://www.cnnbrasil.com.br/nacional/sptrans-diz-que-foi-alvo-de-ataque-cibernetico-e-teve-dados-cadastrais-vazados/>.

CARRANÇA, Thais. Como a Amazon dominou vendas de livros no Brasil em apenas 9 anos. BBC News Brasil, 2 maio 2023. Disponível em: https://www.bbc.com/portuguese/articles/c4nwprveg0wo.

DATAREPORTAL. Digital 2024: Global Overview Report. [S. l.], 2024. Disponível em: <https://datareportal.com/global-digital-overview>.

DE JANEIRO, R.; MONICA HERZ. Luísa Cruz Lobato Unraveling the cyber security market: The struggles among cyber security companies and the production of cyber (in)security Dissertação de Mestrado. [s.l: s.n.]. Disponível em:

<https://www.maxwell.vrac.puc-rio.br/27784/27784.PDF>.

FAN, Ricardo. Como a ciberguerra global vai impactar a segurança no Brasil. DefesaNet, 16 maio 2025. Disponível em: https://www.defesanet.com.br/cyberwar/como-a-ciberguerra-global-vai-impactar-a-seguranca-no-brasil/.

FELDMANN, Paulo. O assombroso poder das Big Techs na economia e na política dos países. Jornal da USP, São Paulo, 2023. Disponível em: <https://jornal.usp.br/articulistas/paulo-feldmann/o-assombroso-poder-das-big-techs-na-economia-e-na-politica-dos-paises/>.

FORTINET. Attack surface. [S. l.], [2024?]. Disponível em: <https://www.fortinet.com/br/resources/cyberglossary/attack-surface>.

GOOGLE CLOUD. O que é Big Data? [S. l.], [s.d.]. Disponível em: https://cloud.google.com/learn/what-is-big-data?hl=pt-br.

GOOGLE. Como a Google usa os cookies. [S. l.], [2024?]. Disponível em: https://policies.google.com/technologies/cookies?hl=pt-BR.

GOOGLE. Sobre publicidade personalizada. [S. l.], [2024?]. Disponível em: <https://support.google.com/google-ads/answer/2407785?hl=pt-BR>.

IBM. What is a single point of failure (SPOF)?. In: IBM Documentation: z/OS Version 3.1.0. [S. l.], 2024. Disponível em: <https://www.ibm.com/docs/en/zos/3.1.0?topic=data-what-is-single-point-failure>.

INTERCEPT BRASIL. Como a Netflix e as redes sociais mudaram a internet. [S. l.], 2020. Disponível em: <https://www.intercept.com.br/2020/09/14/internet-netflix-redes/>.

INSTITUTO TRICONTINENTAL DE PESQUISA SOCIAL. Big Techs e os desafios atuais para a luta de classes. [S. l.], n. 46, nov. 2021. Disponível em: https://thetricontinental.org/wp-content/uploads/2021/11/20211026_Dossier-46_PT_Web.pdf.

KHANAL, S.; ZHANG, H.; TAEIHAGH, A. Why and How Is the Power of Big Tech Increasing in the Policy Process? The Case of Generative AI. Policy & Society (Print), v. 44, n. 1, 27 mar. 2024.

LE MONDE DIPLOMATIQUE BRASIL. Big Techs desafiam a democracia e favorecem a extrema direita. [S. l.], 2023. Disponível em: <https://diplomatique.org.br/big-techs-desafiam-a-democracia-e-favorecem-a-extrema-direita/>..

LEVINE, Yasha. Surveillance Valley: the secret military history of the Internet. New York: PublicAffairs, 2018.

MICROSOFT AZURE. What is the cloud?. [S. l.], [2024?]. Disponível em: <https://azure.microsoft.com/pt-br/resources/cloud-computing-dictionary/what-is-the-cloud>.

MOROZOV, Evgeny. Big Tech: a ascensão dos dados e a morte da política. São Paulo: Ubu Editora, 2018.

MOTORYN, Paulo. Nikolas gastou R$ 750 mil na Meta para vender curso. Eu comprei.

The Intercept Brasil, 3 jul. 2025. Disponível em: https://www.intercept.com.br/2025/07/03/nikolas-meta-curso-destra/.

OUTRAS PALAVRAS. O braço armado das Big Techs. [S. l.], 2023. Disponível em: <https://outraspalavras.net/tecnologiaemdisputa/o-braco-armado-das-big-techs/>.

TECHNOLOGY REVIEW. Data for a new enlightenment. [S. l.], 2019. Disponível em: <https://www.technologyreview.com/2019/06/14/65678/data-for-a-new-enlightenment/>.

THE DECISION LAB. Social physics. [S. l.], [2024?]. Disponível em: <https://thedecisionlab.com/reference-guide/psychology/social-physics>.

TOTVS. Política de Privacidade. Blog da TOTVS, 2024. Disponível em: <https://www.totvs.com/blog/gestao-para-assinatura-de-documentos/politica-de-privacidade/>.

ULNICANE, I.; ADEN, A. Power and politics in framing bias in Artificial Intelligence policy. Review of Policy Research, v. 40, n. 5, 28 jun. 2023.

ZUBOFF, Shoshana. A era do capitalismo de vigilância. [S. l.], 2019. Disponível em: <https://nae.com.pt/wp-content/uploads/A-Era-do-Capitalismo-de-Vigilancia-Shoshana-Zuboff.pdf>.