PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO

FACULDADE DE CIÊNCIAS SOCIAIS

Julia Manoel Agostinho

O processo de securitização da tecnologia por Israel e seus efeitos nos estudos de Segurança Internacional: uma análise sobre o caso Pegasus.

Bacharelado em Relações Internacionais

SÃO PAULO

2025

Julia Manoel Agostinho

O processo de securitização da tecnologia por Israel e seus efeitos nos estudos de Segurança Internacional: uma análise sobre o caso Pegasus.

Trabalho de Conclusão de Curso apresentado à Banca Examinadora da Pontifícia Universidade Católica de São Paulo, como exigência parcial para obtenção do título de BACHAREL em **Relações Internacionais**, sob a orientação do Prof. Dr. **David Magalhães.**

SÃO PAULO

2025

AGRADECIMENTOS

Em primeiro lugar, gostaria de agradecer meus pais, Adriana e Wilson, meus primeiros professores. Obrigada por priorizarem minha educação acima de absolutamente qualquer outra coisa, por acreditarem em mim quando eu mesma não o fiz e especialmente por estarem presentes em todos os momentos importantes da minha vida. À minha mãe, minha maior inspiração - você me ensinou o que é ser mulher. Enfrentou uma jornada exaustiva para realizar o sonho de se formar na faculdade, mesmo depois de casada e com uma filha. Não há exemplo maior de perseverança e resiliência, e por mais que eu não diga com frequência, espero que saiba o quanto tenho orgulho de ser sua filha. Ao meu pai, que primeiro me ensinou a paixão pela política, pelo estudo e pelo mundo - além, é claro, dos conceitos básicos de física, os quais eu nunca fui capaz de entender inteiramente. Obrigada por sempre colocar minhas vontades e necessidades acima das suas próprias, por me entender e me amar por inteiro e por nunca, em hipótese alguma, ser ausente.

Também gostaria de agradecer aos meus avós, que foram minha segunda casa e em parte responsáveis pela pessoa que sou hoje. À minha vó Lourdes e meu vô Wilson, que infelizmente se foram cedo - espero que se orgulhem e torçam por mim em espírito, como o fizeram em vida. Seu amor à vida, à família e às viagens será lembrado eternamente por seus netos. Vocês teriam amado acompanhar minhas aventuras na Europa. À minha vó Maria e meu vô Dional, obrigada por serem o principal alicerce dos meus pais na minha criação. Minha mãe jamais conseguiria finalizar a faculdade sem que vocês cuidassem de mim, me buscando da escola, preparando meu almoço e me colocando para dormir enquanto meus pais trabalhavam e estudavam. Obrigada também por rezarem pela minha felicidade e sucesso sempre. Não sou religiosa, mas acredito que muito do que conquistei foi em decorrência disso.

Às minhas amigas conterrâneas, Isabela, Giovana e Isabella. Com vocês aprendi sobre a leveza de uma amizade cultivada na infância, e em especial que ela independe do tempo e do lugar para permanecer forte. Seja em São Paulo, Sorocaba, Botucatu ou Ribeirão Preto, sei que permanecemos unidas torcendo pelo sucesso da outra, comemorando juntas cada conquista e chorando cada derrota. Que nossos laços se tornem ainda mais fortes e nos permitam comemorar muitos outros momentos importantes de nossas vidas adultas em companhia.

As amigas também puquianas Carol, Emanuelle, Beatriz, Milena e Yasmin. Que felicidade dividir um período tão importante de nossas vidas com pessoas tão especiais. A

graduação pode ser cansativa e degradante, mas graças a vocês, esses quatro anos da minha vida foram tão felizes e cheios de aprendizados, que não guardo arrependimentos. Obrigada por todos os trabalhos em grupo, pelas voltinhas nos corredores, pelas risadas na prainha e pelas biritas no Paraty. Para além disso, obrigada por serem pessoas das quais eu tenho certeza que continuarão na minha vida agora que a Universidade chegou ao fim.

A Lille e todas as pessoas incríveis que conheci lá, em especial Bruna, Carol, Manuella e Samara. Citando Guimarães, os outros eu conheci por ocioso acaso, vocês eu encontrei porque era preciso.

Por fim, agradeço àqueles que efetivamente tornaram possível esses quatro anos - os professores do curso de Relações Internacionais da PUC SP. Obrigada aos Professores Doutores Rodrigo Amaral e Bruno Huberman, por me introduzirem aos estudos sobre Oriente Médio e Palestina, o que me inspirou na escolha do tema deste trabalho. Agradeço também à Professora Doutora Priscila Villela, por me apresentar os estudos sobre segurança pública e me auxiliar com referências que enriqueceram o presente estudo. Ao Professor Doutor Arthur Murta, obrigada pelas aulas, que considero especialmente revolucionárias no campo das Relações Internacionais, e pelo companheirismo e amizade, em especial durante este último ano. Finalmente, não posso deixar de agradecer ao Professor Doutor David Magalhães, que me orientou nesta longa jornada. Obrigada pela atenção, pelo cuidado e por todos esses anos de aprendizado na PUC. Sua presença é marcante e sua falta será sentida por todos os seus alunos - e que sorte a minha ter sido uma delas. Lhe desejo muito sucesso e felicidade nesse seu novo ciclo, certa de que ainda nos reencontraremos.

São muitas pessoas e lugares diferentes que contribuíram para a conclusão deste trabalho. Eu poderia mencionar a gentil garçonete da cafeteria que frequentei quase toda semana para escrever enquanto apreciava um café superfaturado, ou a atenciosa bibliotecária da PUC que me ajudou a encontrar os livros físicos que usei de referência para estudo e escrita deste documento. Dessa vez, porém, quero variar um pouco e agradecer alguém cujo reconhecimento quase sempre é ignorado inconscientemente. Obrigada, Julia, por continuar e acreditar no potencial desse estudo - imperfeito, assumo - mesmo em meio a bloqueios criativos e desconfianças acerca de sua qualidade. Nessa jornada, a lição mais importante que aprendi foi a de que a única forma de escrever é escrevendo. A escrita, como a vida, se aprende em gerúndio. Por isso, obrigada por não desistir.

RESUMO

O presente trabalho tem como objetivo analisar a securitização da vigilância e da cibersegurança no contexto dos estudos de área de Segurança Internacional contemporânea a partir de um estudo de caso do *spyware* Pegasus, desenvolvido pela empresa israelense NSO Group. A pesquisa parte da hipótese de que o aparato tecnológico israelense é difundido no mercado global de segurança como resultado de um processo histórico de militarização e ocupação colonial, exportando esse novo modelo de segurança especialmente no espaço digital. Assim, busca-se compreender como a lógica colonial e neoliberal transformam a vigilância em mercadoria securitária e consolida um modelo de governança baseado no tecno-autoritarismo, ao passo que o caso israelense evidencia a consolidação de um modelo global de governança securitária através do colonialismo digital, que combina tecnologia, dominação e lucro.

Palavras-chave: Israel; Segurança Internacional; Pegasus; tecnologia; vigilância.

ABSTRACT

This paper aims to analyze the securitization of surveillance and cybersecurity within the context of contemporary International Security studies, using a case study of the Pegasus spyware, developed by the Israeli company NSO Group. The research hypothesizes that Israeli technological apparatus is widespread in the global security market as a result of a historical process of militarization and colonial occupation, exporting this new security model, especially in the digital space. Thus, it seeks to understand how colonial and neoliberal logic transforms surveillance into a security commodity and consolidates a governance model based on techno-authoritarianism, while the Israeli case highlights the consolidation of a global security governance model through digital colonialism, which combines technology, domination, and profit.

Keywords: Israel; International Security; Pegasus; technology; surveillance.

SUMÁRIO

INTRODUÇÃO

Em meados de 2021, o jornal americano *Washington Post* revelou uma das maiores investigações jornalísticas sobre espionagem digital do século XXI, o "Pegasus Project". A apuração, feita a partir de relatórios desenvolvidos pelo *Citizen Lab*, expôs que o software israelense *Pegasus* da NSO Group havia sido utilizado para monitorar jornalistas, ativistas e líderes políticos em dezenas de países. A descoberta trouxe à tona questionamentos éticos e políticos sobre os limites de ferramentas de segurança em um mundo cada vez mais globalizado e dependente de tecnologias digitais. Nesse sentido, o desenvolvimento de ferramentas de segurança e vigilância, sobretudo a partir do século XXI, representa um novo momento nos estudos da área de Segurança Internacional - dessa vez na esfera digital.

O escândalo envolvendo o Pegasus evidencia um fenômeno que ultrapassa a dimensão técnica da cibersegurança - a transformação da vigilância em instrumento de poder político e econômico. No caso israelense, as raízes do aparato tecno-militar de segurança estão essencialmente vinculadas a um processo militar e colonial, onde o desenvolvimento de tecnologias de defesa e vigilância testadas no território palestino possibilitaram sua comercialização no mercado internacional. Em parceria com agentes do Estado, o papel de empresas privadas na execução dessas práticas está cada vez mais evidente e atua na reafirmação de uma ordem neoliberal que contribui para um regime global de segurança controverso e assimétrico.

É nesse sentido que surgem questões centrais acerca dos estudos de área de Relações Internacionais na contemporaneidade. Como o processo de securitização tecnológica atua no desenho e redirecionamento dos estudos de segurança internacional, ao mesmo tempo que redefine as relações entre Estados, setores privados e indivíduos? Para além disso, focando no caso israelense, como o Pegasus exemplifica de forma paradigmática a instrumentalização política e econômica da vigilância digital em nome da segurança?

O presente estudo parte dessas questões para investigar o processo de securitização do aparato tecnológico de segurança por Israel e os meios pelos quais ele atua, o que contribui para o debate teórico e empírico da segurança internacional. A pesquisa propõe que a segurança, tradicionalmente vinculada à defesa militar e ao Estado, é reinterpretada à medida que a tecnologia passa a assumir um papel central na legitimação de ameaças e na reprodução de estruturas de poder. Legitimado por atos discursivos e sob uma ótica mercadológica, ferramentas tecnológicas de vigilância são convertidas em produtos lucrativos de exportação e

exploração, quando deveriam ser supostamente utilizados para proteção e segurança da população.

O objetivo deste estudo se baseia na tentativa de compreensão de implicações políticas e econômicas acerca do avanço do desenvolvimento e utilização de tecnologias de vigilância como produtos de um novo modelo de segurança internacional. Nesse sentido, investiga-se o caso isralense dentro de um contexto global de ascensão de regimes autoritários e normalização de práticas de vigilância digital em escala transnacional. Também foi possível, a partir do estudo, contribuir para o debate sobre o papel de atores privados, como grandes corporações e startups tecnológicas, na formulação de políticas de segurança e desenvolvimento tecnológico, embaçando os limites visíveis entre os setores público e privado. Assim, a metodologia utilizada para elaboração deste estudo consiste em uma revisão bibliográfica acerca do debate sobre Segurança Internacional, alinhado com um estudo de caso sobre o software Pegasus, sua cadeia de produção e sua projeção global voltada por meio da exportação para diferentes contextos e utilizações.

Diante disso, o presente trabalho está estruturado em três capítulos principais. O primeiro capítulo apresenta uma fundamentação teórica e dialoga com as contribuições dos estudos de segurança nas Relações Internacionais, em especial a Escola de Copenhagen e os Estudos Críticos de Segurança. A partir disso, o segundo capítulo foi dividido em três seções, onde são realizadas análises sobre o histórico de construção do aparato tecno-militar israelense, a utilização, desenvolvimento e exportação do Pegasus como produto de segurança pública e o debate acerca da testagem desses produtos no laboratório palestino, em uma lógica colonial. Por fim, o terceiro capítulo vincula o debate teórico à questão prática de utilização de tecnologias de vigilância testemunhado no caso Pegasus, evidenciando como o aparato tecnológico israelense se projeta internacionalmente como modelo de governança securitária contemporânea.

1. VIGILÂNCIA E TECNO-AUTORITARISMO: TRANSFORMAÇÕES NA LÓGICA DE SEGURANÇA INTERNACIONAL

O desenvolvimento tecnológico representa, há séculos, uma constante ressignificação das necessidades humanas e a reconfiguração de setores do sistema internacional. Nas últimas décadas, essa evolução foi marcada pelo progresso no setor digital e de comunicações, sendo a internet o maior exemplo disso, responsável por intensificar o processo de globalização e possibilitar uma hiperconectividade internacional. Esse avanço gerou, como consequência direta, a oferta de uma maior digitalização de serviços nas mãos de empresas privadas e o desenvolvimento de tecnologias de vigilância e cibersegurança. Entretanto, a utilização dessas ferramentas de forma irregular e contínua apresenta ameaças para a segurança que cruzam a fronteira digital, podendo resultar em crises diplomáticas de difícil controle.

O conceito de segurança, no campo acadêmico das Relações Internacionais, esteve histórica e categoricamente associado à capacidade militar do Estado em reagir a ameaças externas e garantir a proteção de sua soberania nacional. Escritores da escola realista como Morgenthau e Carr defendem o papel central do Estado na promoção da segurança doméstica e integridade territorial (MORGENTHAU, 2003; CARR, 2001), enquanto a escola neorrealista o interpreta como uma fonte ofensiva de maximização de poder de acordo com a lógica do sistema internacional anárquico (MEARSHEIMER, 2001). O conflito armado e a militarização do Estado, portanto, eram considerados a base dos estudos envolvendo segurança e balança de poder internacionais.

Essa premissa já começou a ser questionada durante a Guerra Fria pelos Estudos de Paz e outras escolas, que alegam uma cooptação do debate acadêmico de segurança pelos Estados Unidos e Europa, além de denunciar estruturas de poder que reproduzem a violência cotidiana doméstica. Nesse sentido, essa reação à visão tradicional e exclusivamente militarista da segurança optou por englobar princípios do pacifismo e voltados a uma paz positiva com justiça social, cooperação internacional e respeito aos direitos humanos (GALTUNG, 1969). Apesar de ser considerado muito idealista, essa discussão foi fundamental ao abrir espaço para uma proposta de ampliação da abordagem teórica de segurança apresentada pela Escola de Copenhague, a partir dos anos 1990. O fim da era bipolar e a ampliação de ameaças transnacionais como o crime organizado e o terrorismo, aliados ao avanço da influência construtivista, resultaram em uma interpretação mais abrangente no conceito de segurança internacional. Nesse sentido, para Buzan, Waever e Wilde (1998), o setor militar não seria a única ferramenta estatal utilizada na aplicação de

segurança e poder, como defendiam seus predecessores realistas - esses conceitos abrangem também os campos político, econômico e social.

Além disso, os autores dessa escola também defendem que a segurança pode ser considerada um "ato discursivo", ou seja, construída através de um discurso que gera medo e insegurança. Nesse sentido, uma ameaça pode ser construída socialmente e institucionalizada por atores securizantes através de dispositivos estatais e governamentais, como propostas legislativas, atuações políticas e discursos públicos. Uma vez que essa narrativa é colocada em prática, ela pode legitimar medidas excepcionais e extremas com a justificativa de garantia da segurança nacional. Esse processo é conhecido por securitização (BUZAN; WAEVER; DE WILDE, 1998) e permite compreender como medidas abusivas adotadas por Estados muitas vezes são justificadas em prol de um "bem maior". Quando essa discussão é trazida para o campo da cibersegurança, o cenário se torna ainda mais crítico, já que a detecção dessas medidas adotadas no campo digital pode ser mais dificultosa.

A partir disso, é possível compreender como esse discurso pode alimentar a legitimação da vigilância cibernética pelo Estado. Frente a ameaças modernas como o risco de ataques terroristas, por exemplo, que também pode ser considerado um medo estratégico alimentado por agentes estatais (STAMPNITZKY, 2013), a utilização de tecnologias de vigilância e monitoramento é feita, frequentemente, atrelada a uma retórica de proteção nacional. Dessa forma, as ferramentas de vigilância cibernética deixam de ser apenas um instrumento de defesa do Estado e se transformam em instrumentos políticos estratégicos de controle de um governo. Assim, com frequência, a exceção se torna regra, e os alvos deixam de ser ameaças estatais e passam a ser políticos - opositores do governo, jornalistas, políticos e até governos internacionais.

Em contraponto, os estudos críticos de segurança, com grande influência do construtivismo da Escola de Frankfurt, inauguram os anos 1990 com uma nova abordagem teórica sobre a segurança internacional. Ao contrário da Escola de Copenhague, os autores críticos defendem uma análise emancipatória da segurança, com foco no indivíduo como referência final desse conceito, visto que "os Estados são provedores de segurança pouco confiáveis e muito diversos para fornecer 'uma teoria abrangente da segurança' " (BOOTH, 1991, p. 319-320). Ao tecer críticas à análise elitista e estadocêntrica da Escola de Copenhague, portanto, a teoria crítica permite compreender a segurança tradicional como uma ferramenta de dominação, passível de premissas que precisam ser repensadas e centralizando o debate na emancipação do indivíduo perante as estruturas opressoras do Estado.

Assim, os estudos críticos defendem uma segurança internacional cuja referência está centralizada no indivíduo e na sociedade. Para Jones (1995), a insegurança ambiental, alimentar e econômica representam uma ameaça muito mais real e atual para o homem moderno do que uma possível guerra ou conflito transnacional e, por isso, devem ser tratadas com equivalência ou até maior interesse pelo Estado e pelos estudos de segurança. Nesse sentido, a teoria crítica defende um fluxo de segurança que deriva do indivíduo e só então se expande a nível global, tornando toda a comunidade emancipada e realmente segura.

No entanto, essa conduta estatal não ocorre na prática, e assim é possível interpretar que a maioria dos Estados são, na realidade, os maiores geradores de insegurança, ao invés de estabilidade e prosperidade. Essa análise é agravada ao analisar o papel da estrutura econômica Neoliberal presente dentro deste Estado que pressiona o indivíduo. De acordo com Booth (2007), o século XXI deve passar por inúmeras crises políticas, ambientais e humanitárias uma vez que a população continua presa às amarras da insegurança. Ao analisar a aliança entre o Estado e o sistema econômico Neoliberal, é possível compreender que não é do seu interesse promover a estabilidade e a emancipação do indivíduo pois, ao contrário disso, a insegurança é lucrativa para ambos e mercantilizada a nível transnacional, conforme será aprofundado a seguir.

Nessa lógica, a autora estadunidense Shoshana Zuboff defende um novo momento histórico do capitalismo, onde a vigilância digital exerce um papel central na manutenção da segurança pública. De acordo com a autora, a internet, os domínios online, as redes sociais e todo esse amplo espaço cibernético construído pelas *big techs* e empresas privadas cibernéticas e de tecnologia no século XXI representam uma nova forma de domínio inteligente sobre o ser humano onde a coerção e o controle são exercidos com finalidades meramente comerciais, no qual o produto somos nós, os usuários. Assim, Shoshana infere que "o capitalismo de vigilância reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais" (ZUBOFF, 2021, p. 22), ou seja, o comportamento humano neste espaço cibernético é extraído, estudado e comercializado a agentes privados como produto de predição de comportamentos futuros dos usuários. A mineração desses dados é um processo utilizado para descobrir tendências, padrões e fatores chaves de comportamento dos usuários que podem resultar em vantagens estratégicas e competitivas para o mercado consumidor dessas práticas, não apenas seguindo o comportamento humano já estabelecido mas também moldando-o e reorientando-o a uma conduta direcionada e favorável ao mercado tecnológico e neoliberal. Dessa forma, a

vigilância digital se torna um meio instrumental do Estado Neoliberal automatizar e modificar decisões humanas sem coerção direta e emprego de força bruta.

A instrumentalização da ferramenta digital pode ser compreendida, assim, como uma forma de transformar o controle do Estado perante sua população em uma certeza total, pois seu comportamento já está pré-definido. Regimes totalitários clássicos, como o nazismo, utilizavam de meios de coerção direta pela força como censura, prisões e mortes com o objetivo de dominação absoluta do Estado sobre a sociedade e todos seus aspectos comunitários. Assim, o totalitarismo elimina o discurso emancipatório social da segurança e garante o poder do Estado através do controle coercitivo de sua população. Na era da vigilância, por outro lado, uma nova forma de controle não coercitivo se estende através do mercado privado da tecnologia, atrelado à previsibilidade humana garantida pela coleta consentida de dados comportamentais dos usuários. Nesse sistema, o controle total pelo Estado não é exigido, uma vez que esse mercado capitalista manipulativo prevê o comportamento e reduz a autonomia de escolha do indivíduo, transformando-o em uma certeza já moldada previamente.

Essa forma de privatização da política pública e mais especificamente da segurança atrelada aos meios digitais foi especialmente abordada nos trabalhos dos franceses Antoine Vauchez e Pierre France (2020). Na obra, os autores analisam como agentes privados alinhados a uma ideologia neoliberal penetram o aparato estatal e lá se institucionalizam, parasitando todo o mecanismo do Estado e reconfigurando-o de dentro para fora, de forma a representar unicamente interesses de elites econômicas do mercado privado. Assim, uma "República Neoliberal" é edificada, e os limites entre as atuações pública e privada do Estado são dissipadas, o que o leva a pender para as lógicas do mercado em uma governança público-privada mais vinculativa e conectada, onde decisões políticas e *policymakers* preocupados com a segurança pública são gradualmente substituídos por um comportamento neoliberal e mercado-cêntrico.

Portanto, é possível inferir até aqui que o comportamento humano deixa de ser alvo de domínio apenas do Estado, e ambos são capturados pela lógica do mercado privado, cujo interesse é expandir cada vez mais sua área de influência. Em um mundo cada vez mais globalizado e tecnológico, é justo pensar que o desenvolvimento de tecnologias de vigilância representa uma vantagem estratégica não só econômica e social, mas sobretudo política. O avanço das *big techs* e de sistemas de informação e vigilância comprovam a inserção do setor privado de tecnologia no Estado e em discussões políticas. O maior e mais recente exemplo

claro dessa dinâmica foi a presença de gigantes da tecnologia como Mark Zuckerberg, Jeff Bezos, Sundar Pichai e Elon Musk, CEOs bilionários de grandes empresas do setor tecnológico, na posse do presidente americano Donald Trump em 2024, sendo o último inclusive chefe do Departamento de Eficiência Governamental do governo. Esse processo permite deduzir que tais tecnologias incorporam relações de poder hierárquicas e políticas favoráveis àqueles que lhes interessa, ou seja, não são neutras em sua funcionalidade (WINNER, 1999).

Nesse sentido, sociedades e governos autoritários geram, por conseguinte, tecnologias igualmente autoritárias (MUMFORD, 1964). Ferramentas tecnológicas voltadas para o controle, vigilância e dependência humana são empreendidas por aquela mesma República Neoliberal liderada por uma elite econômica desinteressada pelo papel emancipador da segurança pública. Ainda que sob um pretexto democrático, essas tecnologias representam técnicas autoritárias que são normalizadas pelo próprio usuário na sociedade capitalista moderna, reproduzindo a dominação sem uma violência explícita. Essa racionalidade tecnológica, já citada no passado por Marcuse (1988) em um contexto industrial, agora mascara relações de poder entre Estados e elites econômicas neoliberais reforçadas por tecnologias digitais, que por sua vez são apresentadas a priori como neutras e necessárias para o combate a ameaças externas.

Tendo em vista essa prerrogativa pessimista da tecnologia moderna, como então o contexto político, social e militar do Estado influenciam no desenvolvimento tecnológico da sociedade digital moderna? De acordo com a abordagem dos estudos de ciência e tecnologia de MacKenzie e Wajcman (1999), o funcionamento de novas tecnologias estaria inevitavelmente conectado a contextos políticos e institucionais, reforçando assim essa estrutura de poder hierárquica. As novas ferramentas tecnológicas e a sociedade, portanto, fazem parte de uma cadeia simbiótica onde uma alimenta a outra - enquanto a tecnologia é elaborada de acordo com necessidades e valores sociais, ela também reafirma estruturas de poder neoliberais e coloniais, além de interesses geopolíticos e econômicos.

Essa abordagem, portanto, permite compreender como tecnologias modernas como a inteligência artificial, os algoritmos de segurança, os sistemas de rastreamento e sobretudo os softwares de vigilância podem ser analisadas como armas cibernéticas que reproduzem estruturas de poder globais e influenciam nas relações internacionais e na balança de poder do sistema internacional. Nesse sentido, a cadeia de produção tecnológica captura estruturas coloniais de poder visíveis na sociedade, e as reproduzem internamente de forma

automatizada, aplicando por exemplo padrões racistas de detecção de ameaças. Ruha Benjamin (2019) chama de "Novo Código Jim Crow" essas novas tecnologias de segurança e vigilância, em referência ao conjunto de leis racistas impostas pelo governo estadunidense no final do século XIX. Segundo a autora, os algoritmos modernos dessas ferramentas são projetados e aplicados a partir de um sistema global embranquecido, normalizando e institucionalizando uma discriminação digital muitas vezes invisível à primeira vista. A nível internacional, essa discriminação não é voltada apenas a indivíduos racializados e marginalizados, mas também a sociedades inteiras e, ainda, Estados fragilizados.

Em complemento a isso, o uso dessas tecnologias, sobretudo na área da segurança pública e internacional, também é utilizado politicamente para reforçar estruturas autoritárias de poder global. A utilização da inteligência artificial, por exemplo, reforça essas estruturas opressivas e está frequentemente relacionada ao colonialismo de dados (CRAWFORD, 2021), no qual países desenvolvidos do norte global e *big techs* extraem dados de populações periféricas, tornando as ferramentas tecnológicas um instrumento de vigilância transnacional originado de governos autoritários.

Como será examinado mais profundamente no próximo capítulo, um exemplo claro dessa dinâmica é a utilização dessas tecnologias por Israel em áreas palestinas ocupadas. O governo, aliado ao mercado militar israelense, utiliza tecnologias militares que incluem ferramentas de reconhecimento facial, monitoramento por satélites e drones, sistemas de rastreamento e de controle de fronteiras, vigilância digital, entre muitas outras que consistem na compreensão e controle de comportamentos humanos na região. Como objeto deste estudo, será explorado como essas tecnologias desempenham um papel fundamental de influência na guerra e nos direitos humanos daquela população e, assim como aponta Crawford, reproduzem relações de poder e autoridade coloniais.

Ainda nessa conjuntura, é interessante analisar como a internet, as plataformas digitais e a tecnologia como um todo se tornam um ponto crucial de debate sobre segurança no Oriente Médio a partir da Primavera Árabe, no início dos anos 2010. Em um momento de mobilização social contra governos autoritários e repressivos, a tecnologia foi adotada como uma ferramenta de libertação democrática, quando antes era vista apenas como refúgio para o lazer e entretenimento. Assim, as plataformas digitais se tornaram vitrine global da violência estatal exposta pelos usuários, além de meio de organização descentralizada de manifestações e mobilizações contra essa estrutura autoritária do governo. Todo esse processo recebeu o suporte de redes de apoio e solidariedade transnacionais, o que impulsionou uma resposta

rápida destes Estados. Porém, a reação autoritária não tardou, e o investimento estatal em tecnologias sofisticadas de repressão digital cresceu gradualmente desde então por esses governos. De acordo com Ronald Deibert (2015), a Primavera Árabe marcou um ponto de inflexão na reação digital do Estado e a transição de um controle defensivo para um controle ofensivo. Nesse sentido, em um primeiro momento, a reação veio através de uma defesa passiva baseada em bloqueio de plataformas digitais e censuras, de forma a conter a expansão dessas mobilizações e evitar as revoltas contra o governo no território doméstico. Em uma medida extrema, o governo egípcio chegou a cortar o acesso nacional à internet por cinco dias em 2011 visando conter o fluxo de informações compartilhadas. Entretanto, a utilização de VPNs, redes Tor, ferramentas *peer-to-peer* e aplicativos de comunicação cifrada surgiram como forma de resistência da população à censura imposta pelos governos, o que gerou apoio da mídia e de organizações internacionais em um efeito bumerangue.

A repressão visível do aparato estatal frente a essas ameaças foi lida como um sinal de enfraquecimento do governo e ineficácia das estratégias contra insurgentes digitais adotadas contra os usuários. Diante disso, o Estado se viu obrigado a assumir táticas legais e institucionalizadas de combate às mobilizações (DEIBERT, 2015), entre elas a elaboração e adoção de legislações amplas que criminalizam a postagem e compartilhamento de publicações de opositores políticos, a judicialização da repressão digital, a inauguração de agências de cibersegurança acusadas de censura e, sobretudo, a parceria com *big techs* para monitoramento de mídia, controle de páginas e conteúdos de opositores e captura de dados de usuários.

Nesse sentido, com a cooptação desse aparato judicial e digital, os governos autoritários abriram caminho para uma nova forma de controle ofensivo do ambiente digital e cibernético. A vigilância proposta por Zuboff (2020) foi instaurada pelo Estado com o apoio e atuação direta de grandes empresas, normalizando casos de espionagem digital de opositores, ataques hackers, monitoramento ostensivo por plataformas digitais e desenvolvimento tecnológico voltado para a neutralização da desordem digital e vigilância algorítmica. Essas medidas não são reconhecidas como censura, uma vez que a atuação desses usuários não é interrompida ou cessada, porém é possível inferir que o Estado encontrou, nessas tecnologias digitais, novos instrumentos de poder e controle autoritário, que influem em uma repressão transnacional.

Portanto, diante do exposto, é possível concluir que a tecnologia vem sendo utilizada por Estados como tática de controle e poder político não apenas no âmbito doméstico como

também internacional. Essa medida vem sendo adotada como parte de uma estratégia mais ampla e histórica, que consiste no desenvolvimento tecnológico como um novo braço da segurança, que pode estar atrelada ao setor militar, e que não mais volta sua atenção apenas para ameaças externas como também a agentes domésticos e aliados de forma preemptiva. Com o objetivo de maximizar seu poder e lucro e prever comportamentos futuros, ferramentas de vigilância são desenvolvidas e comercializadas sem qualquer regulamentação e indicam o princípio de um futuro tecno-autoritário mundial liderado pelo Estado e grandes empresas.

2. MERCADO SECURITÁRIO, COLONIALISMO DIGITAL E O CASO PEGASUS: RAÍZES DA VIGILÂNCIA EM ISRAEL E A CONSTRUÇÃO DE UM MODELO SECURITÁRIO TRANSNACIONAL

O presente capítulo terá como foco apresentar ao leitor o objeto de estudo desta pesquisa, o *spyware* Pegasus, produto da crescente produção tecnológica israelense, através de uma perspectiva crítica e analítica sobre o funcionamento desse sistema. É imprescindível pontuar, nesse sentido, que o desenvolvimento e implementação desse programa derivam de um longo processo de fortificação e autossuficiência do complexo industrial tecno-militar de Israel, construído a partir de um contexto histórico e colonial. Portanto, analisaremos a princípio a evolução da produção nacional desse setor, sustentada por um verdadeiro laboratório de testagens deste arsenal, para então compreender o avanço tecnológico promovido pelo Estado sionista aliado a grandes empresas de tecnologia e a exportação de seus produtos de forma crescente e alarmante.

2.1 O histórico da produção tecno-militar de Israel e seu legado

O desenvolvimento do complexo militar de Israel possui raízes históricas que remontam ao período anterior ao estabelecimento do Estado israelense, entre os anos 1920 e 1940, atrelado à atuação de organizações paralelas e clandestinas ao mandato britânico no território palestino. De acordo com Uzi Rubin (2017), engenheiro especialista em defesa de mísseis nas Forças de Defesa de Israel e altamente ligado ao *establishment* militar israelense, a atuação de organizações paramilitares judaicas ligadas à Agência Judaica, como a *Haganá*, formada majoritariamente por milícias locais para defesa de assentamentos judeus, impulsionou o desenvolvimento de oficinas clandestinas na Palestina e representa os primeiros passos do que hoje conhecemos como um grande complexo industrial de produção bélica israelense, com conexões transnacionais e altamente tecnológico.

Além da *Haganá*, outras organizações paramilitares judaicas também contribuíram para esse processo. O *Irgun*, também conhecido pelo acrônimo *Etzel*, foi uma organização que nasceu como uma dissidência da Haganá ao legitimar operações de represália contra britânicos e árabes, enquanto o *Lehi* atuou a partir de uma doutrina ainda mais radical. Essas organizações nasceram com um suposto propósito de defesa da comunidade judaica da região, munidos com armas leves de produção local clandestina ou frutos de contrabando. A prática, contudo, evoluiu para o desenvolvimento de explosivos e granadas de mão, e posterior uso de

sub metralhadoras, morteiros e munições pesadas (RUBIN, 2017). Aos poucos, essas organizações também se mostraram cada vez mais adeptas a um nacionalismo judeu sionista e passaram a atacar não apenas o mandato britânico na região, como também a comunidade com a qual compartilhavam aquele território. O Massacre de *Deir Yassin* foi um episódio marcante que exemplifica essa prática, no qual cerca de 120 civis palestinos - incluindo mulheres, crianças e idosos - foram executados sumariamente em uma ação conduzida pelo *Irgun* e pelo *Lehi* em abril de 1948 (KHALIDI, 1992), em meio a um plano maior de expulsão forçada que garantiria a criação do Estado nacional judeu, o Plano Dalet ou Plano D (PAPPE, 2006).

Apesar desses fatores controversos, a resolução das Nações Unidas de 1947 (ONU, 1947) e a independência de Israel em maio de 1948 marcaram um ponto de inflexão na atuação desses grupos paramilitares. À medida que eram associados a movimentos insurgentes e clandestinos durante a ocupação britânica na região, essas organizações - em especial a Haganá - foram convertidas ao papel de principal força militar judaica do Estado de Israel, auxiliando tanto na expulsão da população palestina da região para consolidação dos propósitos sionistas, quanto na repressão aos países árabes durante a Primeira Guerra Árabe-Israelense. Nesse sentido, em um esforço conjunto de unificação do comando militar dos grupos paralelos atuantes na região e formação de um Exército israelense fortalecido, o governo provisório criou oficialmente as Forças de Defesa de Israel (IDF) dias após a independência. Com isso, a Haganá foi legalizada e incorporada quase que integralmente na IDF (RUBIN, 2017), o que possibilitou o fornecimento de uma base organizacional desenvolvida aos poderes do Estado, assim como um comando militar e tropas locais extremamente experientes e habituadas ao combate contra populações já segregadas naquele território.

Atrelado a essa militarização do Estado recém estabelecido, Israel passou por um momento de consolidação de suas estruturas industriais e científicas no departamento de defesa. Em 1953, o então Primeiro Ministro e Ministro de Defesa David Ben-Gurion começou a esboçar alguns projetos de desenvolvimento e produção bélica que buscavam expandir a indústria militar israelense para suprir as demandas internas das IDF e gerar autossuficiência no setor de segurança do país (UNITED STATES, 1991). Nesse sentido, a consolidação de estatais como a Israel Aerospace Industries (IAI), a principal fabricante aeroespacial de aviação com foco na produção de sistemas espaciais aéreos e astronáuticos, caças e mísseis,

foi essencial para o avanço das IDF e o pontapé inicial para a comercialização de produtos militares israelenses a forças armadas estrangeiras (RUBIN, 2017).

Além disso, o governo israelense investiu fortemente no desenvolvimento científico e tecnológico do país desde o início. Em 1948, por exemplo, foi criado o Rafael, um departamento do Ministério de Defesa de Israel classificado como o corpo científico da IDF e centro de inovação militar, responsável pelo desenvolvimento de novos sistemas de segurança nacionais. Junto com a IAI, o Rafael foi responsável pela criação do Iron Dome, sistema de defesa antimísseis, além do desenvolvimento dos sistemas de mísseis Popeye e Spike, posteriormente exportados para diversos países, e tecnologias navais e aéreas, com o crescimento massivo de investimentos no setor de cibersegurança já nos anos 2000.

Apesar dos investimentos estatais para consolidação doméstica do setor de segurança por Israel, o país ainda se sujeitava a uma forte política de dependência bélica de importações no setor de segurança. Exemplo disso é o Israel Military Industries (IMI), uma indústria clandestina da Haganá que, assim como a organização, foi incorporada ao Estado após a independência e se tornou uma estatal, parte de um programa de industrialização interna financiado pelo governo israelense com assistência americana, dependente sobretudo de aquisições de armas da França, Estados Unidos e Inglaterra (RUBIN, 2017). Em especial, notou-se uma aliança ainda mais forte com a França entre as décadas de 1950 e 1960, onde o país se tornou o principal fornecedor de armas e artefatos militares em uma convergência estratégica contra o pan-arabismo crescente e ameaçador na região, sobretudo no território do vizinho Egito (SHLAIM, 2004). Nesse sentido, o nível de dependência israelense de produtos franceses se tornou altíssimo através do acesso a equipamentos militares avançados como caças, tanques de guerra e tecnologia nuclear (MORRIS, 2001; COHEN, 1998), enquanto a produção local se limitava a produzir armas leves e munições, em complemento às importações. Esse fato possibilitou que Israel modernizasse suas forças armadas de forma acelerada e estruturada, garantindo uma superioridade bélica regional e uma forte aliança com o ocidente a partir das importações.

Contudo, esse cenário sofreu uma mudança significativa após a independência argelina. Com o objetivo de se reaproximar ao mundo árabe, recuperar sua influência no mercado da região e garantir seu acesso ao petróleo, a França passou a adotar uma postura mais equilibrada e diplomática, garantindo relações com os novos Estados árabes após a recente derrota na Argélia. Nesse sentido, às vésperas da Guerra dos Seis Dias, o governo francês liderado pelo General Charles de Gaulle implementou um embargo de armas à Israel,

promovendo um bloqueio imediato do fornecimento de artigos militares como aviões de combate, tanques e peças de reposição já encomendados pelo governo israelense, o que estabeleceu uma rachadura com o principal aliado militar e o maior fornecedor de armas do Estado sionista naquele momento. Este fato representou um divisor de águas para a política de segurança de Israel, demonstrando uma necessidade imediata de autossuficiência bélica do país e inaugurando uma nova política doméstica de independência no setor de segurança estratégica (RUBIN, 2017).

Dessa forma, ao final dos anos 1960 e ao longo dos anos 1970 e 1980, o governo israelense promoveu grandes investimentos em pesquisa e desenvolvimento nacionais, institucionalizando essa prática através da atuação de companhias privadas em programas estatais e de políticas industriais e tecnológicas para inovação (BREZNITZ, 2007). Em 1968, por exemplo, Israel inaugurou um extenso programa político de pesquisa e desenvolvimento (R&D) com financiamento estatal, responsável por colocar as publicações acadêmicas de Universidades israelenses na liderança das listas internacionais, sobretudo em física e engenharia. Essa política de fortalecimento científico nacional também foi direcionada à atuação do Rafael, através de grandes investimentos voltados para os estudos do setor nas IDF e no campo da defesa, possibilitando por exemplo o desenvolvimento nacional de equipamentos militares como o caça Kfir, as lanchas de ataque Sa'ar, os tanques de guerra Merkara e famílias de morteiros e obuseiros (UNITED STATES, 1991).

Em paralelo a isso, o fortalecimento da cooperação tecnológica e militar entre Israel e Estados Unidos também é um fator a ser pontuado como relevante na autonomia bélica do primeiro. A deterioração das relações com a França após o embargo de armas em 1967 acarretou na consequente aproximação com o governo norte-americano através de iniciativas de financiamento na indústria de defesa e cooperação tecnológica e militar (BREZNITZ, 2007). A atuação do *lobby* israelense na política americana, nesse sentido, foi crucial para fortalecer essa aliança ainda nos anos 1970, influenciando profundamente a política externa americana através de financiamento de campanhas e da atuação do American Israel Public Affairs Committee (AIPAC), comitê que representa os interesses israelenses no Congresso americano. Para além disso, desde o início da Guerra de Yom Kippur em 1973, Israel tem sido o maior beneficiário da assistência militar americana, recebendo uma verba securitária anual de cerca de 3 bilhões de dólares de ajuda externa, ainda que com relativas discordâncias acerca da atuação política e militar israelense na região (MEARSHEIMER; WALT, 2007). Assim, os Estados Unidos foram gradualmente substituindo a França no papel de parceiros

militares e tecnológicos de Israel, além de estabelecer uma relação política que fortalece o setor de segurança israelense e exerce influência no equilíbrio de poder da região do Oriente Médio.

Além disso, o protagonismo do setor privado foi sendo cada vez mais encorajado em Israel através de incentivos fiscais, programas de cooperação internacional e apoio a *startups* de setores tecnológicos emergentes. Breznitz cita em sua obra (2007) o exemplo inicial do que hoje é conhecido como o ecossistema *high-tech* operante no país, no qual o Israel Discount Bank, de capital aberto, começou a financiar e investir em iniciativas da Elron Group nos anos 1970, a primeira *holding* de tecnologia de defesa israelense com forte ligação à expertise militar, focada em softwares empresariais e serviços de cibersegurança. Assim, essa aliança abriu espaço para o avanço de *startups* que hibridizam o setor de defesa e o campo civil em paralelo à indústria militar. Nesse sentido, combinando fatores de base científica, *know-how* militar e capital privado, o financiamento israelense a esse processo colocou o país em uma posição de liderança na produção e exportação de softwares e tecnologias de uso civil e militar.

Portanto, apesar de inicialmente dependente de tecnologias e aparato bélico importados de aliados externos, Israel conseguiu desenvolver sua indústria de segurança tecno-militar a partir de investimentos maciços em pesquisa e desenvolvimento, através de financiamentos governamentais e privados. Com isso, a autossuficiência no setor, conforme proposto anteriormente, foi não apenas concretizada com a produção para abastecimento interno, mas também ultrapassada ao colocar Israel como referência mundial em modernização e diversificação militar, possibilitando uma capacidade extra voltada à exportação para regiões da América Latina, Ásia, África e Europa. Conforme pontuou o relatório publicado pelo Escritório de Avaliação Tecnológica do Congresso americano,

> Israel embarcou em um curso altamente ambicioso de expansão, diversificação e modernização de sua indústria de defesa. (...) Consequentemente, no início da década de 1970, a indústria de defesa israelense, que naquela época consistia em muitas corporações privadas e públicas, foi capaz de desenvolver e produzir internamente uma gama de sistemas de armas avançadas. (UNITED STATES, 1991, p.85, tradução própria).[1]

Tendo em vista esse histórico, é possível compreender como Israel redirecionou esse movimento de desenvolvimento tecnológico e militar do cenário doméstico para mercados

[1] "Israel embarked on a highly ambitious course of expanding, diversifying, and modernizing its defense industry. (...) Consequently, by the early 1970s the Israeli defense industry, which by this time consisted of many private as well as public corporations, was able to develop and produce domestically a range of advanced weapons systems."

globais a partir dos anos 1990 e 2000. Em 1987, o país chegou ao marco de 3,5 bilhões de dólares de lucro em exportações bélicas (UNITED STATES, 1991), e dez anos depois, mais de 50% das receitas do setor bélico provinham de exportações (BREZNITZ, 2007). Nesse sentido, apesar do mercado local ter sido crucial para o desenvolvimento tecnológico da indústria israelense, o que se vê é uma expansão estratégica do setor em busca de mercados externos nos últimos trinta anos. Com o recente crescimento das plataformas digitais, o avanço das *high-techs* e a projeção cibernética a nível global, não apenas no âmbito civil mas inclusive e sobretudo no político e militar, percebe-se uma migração da indústria de defesa insraelense também para o ambiente digital, com tanta ou até mais influência quando comparado ao setor bélico.

Nesse contexto, as políticas públicas de R&D no setor de tecnologia ganharam ainda mais projeção no país. A articulação entre as Science and Technology Policies (SeT) e as High-Tech Policies (HTP) foram responsáveis por expandir um conjunto de políticas estratégicas de fomento ao desenvolvimento e inovação do conhecimento científico e tecnológico na indústria *high-tech* e de cibersegurança. As SeT são políticas mais amplas que consistem em programas coordenados pelo governo para fortalecer a base científica do país, como o fomento à pesquisa com altos investimentos universitários, o que cria uma base científica substancial para as políticas high-tech. Um exemplo disso é o Programa Magnet, criado em 1990 pelo *Office of the Chief Scientist* (OCS), que estrutura-se em consórcios entre universidades e empresas privadas. Assim, o governo israelense oferece financiamento parcial enquanto as empresas adquirem a propriedade intelectual dos resultados de pesquisa, mas são obrigadas a compartilhar essas novas tecnologias com todos os membros daquele programa, de forma que o investimento inicial não se concentre em um ator específico mas alcance todo o ecossistema envolvido no processo (BREZNITZ, 2007).

A partir disso, as HTP são um conjunto de medidas voltadas especificamente para o setor da indústria high-tech, almejada como um motor de crescimento no país. Nesse caso, o foco é justamente fomentar a pesquisa aplicada através de estímulos à pesquisa com resultados comerciais, como o apoio a *startups* em conexão com a indústria de defesa - aproveitando a experiência da IAI, do Rafael e da Elbit, por exemplo - e a internacionalização do setor, tornando essa tecnologia um produto voltado para a exportação (RUBIN, 2017). Foi nesse contexto, no início dos anos 2000, que nasceram algumas das primeiras *startups* de tecnologia e cibersegurança em Israel com uso dual - tanto civil quanto militar. Essas empresas não só atendiam à demanda do mercado doméstico, mas rapidamente se destacaram no mercado global, situando Israel como um *hub* de inovação global no setor através de um

complexo industrial e tecnológico extremamente desenvolvido em Tel Aviv, o Silicon Wadi (BREZNITZ, 2007), semelhante ao modelo californiano.

Sendo assim, é possível afirmar que Israel possibilitou uma adaptação estratégica de sua trajetória na indústria de segurança. Rubin (2017) defende a ideia de que, hoje, a indústria de defesa israelense é constituída em essência pela indústria *high-tech*, e seu futuro está na privatização e na exportação, ao mesmo tempo em que segue um processo de integração a mercados internacionais de defesa. A título de comparação, enquanto os Estados Unidos possuem 40% das *startups* de tecnologia do mundo, Israel possui apenas 20%, mas cerca de 35% de todas as empresas unicórnio (LEE, 2013) - isto é, avaliadas em mais de um bilhão de dólares - da categoria são israelenses (VOHRA, 2023), o que demonstra um crescimento descomunal do setor de cibersegurança privada no país. Alinhado a isso, o incentivo fiscal do governo é indispensável nesse processo, uma vez que algumas *startups* recebem até 300 mil dólares de investimento inicial estatal para o desenvolvimento dessas tecnologias, sem necessidade de devolução posterior dessa receita (VOHRA, 2023). Assim, há uma confluência de interesses entre governo e empresas privadas no setor de defesa israelense, possibilitando o suprimento do mercado doméstico e o lucro com o excedente da produção direcionado às exportações, conforme abaixo:

> Embora a maioria das grandes empresas de defesa do mundo seja de propriedade privada, várias grandes empresas israelenses de defesa são de propriedade total ou parcial do governo (...) O governo israelense é o principal cliente da indústria de defesa israelense, adquirindo diversas plataformas e diversos tipos de sistemas de armas para os diferentes ramos das Forças de Defesa de Israel (IDF). Essa aquisição geralmente é uma condição essencial para a exportação de sistemas e plataformas de armas militares israelenses para outros países ao redor do mundo (TISHLER; PINCHAS, 2020, p.33, tradução própria).[2]

Em síntese, é possível concluir que o processo histórico de produção tecno-militar israelense é permeado por contínuas adaptações às transformações políticas, econômicas e estratégicas do cenário internacional para fortalecer a realidade doméstica. Desde um aparato clandestino ligado a grupos paramilitares, Israel transitou da dependência de aliados externos para a autossuficiência de seu complexo militar, e hoje consolida-se como líder em inovações no setor de defesa high-tech e cibersegurança. A expertise derivada do *know-how* militar, os investimentos estatais em pesquisa e desenvolvimento no setor, a crescente atuação de empresas privadas e a integração aos mercados globais, combinados, permitiram o

[2] "While most of the world's large defense companies are privately owned, a number of large Israeli defense companies are owned fully or partially by the government (...) Israeli government is the Israeli defense industry's main customer, procuring various platforms and many types of weapons systems for the different branches of the IDF. This procurement is usually an essential condition for exporting Israeli military weapon systems and platforms to other countries around the world"

aperfeiçoamento de um modelo singular no qual a indústria de tecnologia não apenas sustenta uma superioridade regional, mas também projeta o país como ator central no setor tecno-militar de segurança internacional.

2.2 O caso Pegasus e o NSO Group

A presente seção analisará como opera a indústria de tecnologia de defesa em Israel, com base em um tripé baseado na militarização, privatização e exportação, que sustentam esse ecossistema. Para isso, será feito um estudo de caso sobre o software Pegasus, projetado e implementado pela empresa israelense de ciberinteligência NSO Group, que consiste em um instrumento de vigilância digital usado de forma estratégica na política e vendido para, ao menos, 45 países (MARCZAK et al., 2018). Pretende-se, com essa análise, assimilar a lógica contemporânea da mercantilização da segurança no setor tecno-militar de Israel, além de promover o tensionamento no debate de Estudos de Segurança Internacional, ao passo que a noção de ameaça é deslocada do campo militar clássico para a esfera cibernética e transnacional.

Em primeiro lugar, é preciso destacar que esse grande fomento ao setor privado de tecnologia, conforme pontuado anteriormente, também gerou crescimento na área de cibersegurança. Hoje, estima-se que Israel possui mais de 400 empresas atuantes nesse campo (IVC RESEARCH CENTER, 2016), entre elas a NSO Group, fundada em 2010 por ex-integrantes da Unidade 8200, o principal tentáculo de inteligência cibernética e espionagem digital das IDF. A empresa se apresenta como uma companhia privada desenvolvedora de softwares de ciberinteligência com foco em combate ao crime organizado e terrorismo, fornecendo a governos e agências de segurança tecnologias de vigilância de comunicações de alvos suspeitos. O grupo já figurou entre as empresas de tecnologia mais valorizadas em Israel, com apoio financeiro de investidores externos e vínculo com outras empresas do setor, como a Cellebrite, a Candiru e a Francisco Partners. Este é um exemplo concreto que confirma o fator essencialmente *high-tech* e privatizado da indústria de defesa israelense (RUBIN, 2017), mas também demonstra sua articulação com a expertise das forças militares do Estado.

Com base nesse histórico, em 2011 a NSO Group desenvolveu e lançou o software Pegasus, um spyware que consegue penetrar nos serviços de segurança de dispositivos eletrônicos sem a permissão ou conhecimento do usuário, viabilizando sua vigilância. A infecção ocorre através de um link de exploração que, ao ser clicado, permite a penetração e

instalação do Pegasus no dispositivo. A partir disso, o operador do software pode receber e executar comandos no aparelho, incluindo acesso a senhas, listas de contatos, eventos do calendário, mensagens de texto e chamadas de voz de aplicativos. O operador consegue, ainda, realizar gravações de voz e vídeo ao acionar a câmera e o microfone do dispositivo com o Pegasus, tudo isso sem o conhecimento do alvo. Apesar das preocupações levantadas acerca do uso do software contra a sociedade civil, impactando o direito à privacidade e a proteção de dados pessoais, o diretor e fundador da NSO Group, Shalev Hulio, garantiu a conformidade do produto. De acordo com Shalev, o "produto é licenciado para agências governamentais e policiais com o único propósito de investigar e prevenir crimes e terrorismo. Nossos negócios são conduzidos em estrita conformidade com as leis de controle de exportação aplicáveis." (MARCZAK et al., 2018), o que implicaria, em teoria, em uma utilização restrita e legalmente regulada pelos respectivos governos que optassem pelo seu uso.

Entretanto, entre 2016 e 2018, após inúmeras denúncias do uso indiscriminado e mal intencionado do software, o *Citizen Lab* realizou uma extensa pesquisa que quantificou e mapeou a atuação do Pegasus, possibilitando a identificação de mais de mil endereços IP que indicavam a contaminação a nível global (MARCZAK et al., 2018). O Citizen Lab é um laboratório interdisciplinar com sede na Universidade de Toronto, no Canadá, que aplica um método misto de pesquisa com foco na intersecção de estudos sobre tecnologias de informação, comunicação, direitos humanos e segurança global com base acadêmica nas ciências políticas, no direito internacional e nos estudos de área. Nesse sentido, o grupo investiga temas ligados à espionagem digital contra a sociedade civil, tecnologias e práticas que impactam a liberdade de expressão online, privacidade, segurança, mecanismos de transparência e responsabilização de corporações e agências estatais em relação a dados pessoais e outras atividades de vigilância digital.

Assim, em 2018, o *Citizen Lab* divulgou um relatório detalhando os passos da sua investigação sobre o Pegasus. A princípio, os especialistas em tecnologia da informação e cibersegurança do laboratório desenvolveram o Athena, uma técnica de impressão digital que identifica os rastros deixados pelo Pegasus em diferentes sistemas. O nome foi inspirado na divindade da mitologia grega, cujas histórias dizem que a deusa Atena conseguiu domesticar o cavalo alado Pégaso, tendo-o domado e refreado com uma rédea de ouro. Através da técnica, os pesquisadores do *Citizen Lab* conseguiram agrupar as correspondências de infecção em 36 sistemas distintos, com os quais foi possível identificar o método de ataque,

com *zero-day* e *zero-click exploits*, e a forma de ação do software nos dispositivos, além de compreender melhor seu funcionamento e seus efeitos.

Também foi possível, através da pesquisa, realizar o mapeamento dos dispositivos infectados e de seus operadores a nível global. A partir disso, foi constatada a presença do Pegasus em dispositivos de 45 países diferentes, situados nas Américas, África, Europa, Oriente Médio e Ásia, que teriam sido operados por 33 clientes confirmados da NSO Group, cujos quais podem estar ligados a governos ou agências de segurança estatais. Esses dados implicam na possibilidade de um só operador atuar na vigilância de múltiplos alvos de localidades diferentes, sinalizando uma atividade em cadeia que envolve numerosos atores com diversas motivações para o uso do software. Além disso, também foi possível identificar que, dos 33 operadores apontados, pelo menos dez deles parecem estar direta e ativamente envolvidos em casos de vigilância transnacional, ou seja, utilizando o Pegasus para infectar dispositivos em outros países, que não aquele em que o operador atua (MARCZAK et al., 2018). É importante pontuar que o uso de ferramentas como VPNs e internet via satélite, tanto pelo operador quanto pelo alvo, podem induzir a imprecisões na leitura dos dados levantados pelos pesquisadores, uma vez que a pesquisa utiliza resultados de geolocalização. Apesar disso, o levantamento dessas informações se mostra extremamente relevante na compreensão da possível utilização deste produto em benefício de governos e agências de segurança para fins de vigilância, não apenas de sua própria população, mas também de atores externos.

Nesse sentido, o relatório também lança luz sobre a utilização do spyware em alvos específicos com motivações políticas. Foi descoberto que boa parte dos países que utilizaram o produto dentro do território nacional mantinham históricos duvidosos sobre a preservação dos direitos humanos de seus cidadãos e relatos de comportamento abusivo por parte de serviços de segurança estatais. Nesse sentido, pelo menos seis países com ocorrência significativa de operações do Pegasus - Bahrein, Cazaquistão, México, Marrocos, Arábia Saudita e Emirados Árabes Unidos - já haviam sido vinculados anteriormente ao uso abusivo de spyware para vigiar e atingir sua própria sociedade civil. Em paralelo a isso, também foi identificado que boa parte das infecções foi feita através de servidores que possuíam temas políticos envolvidos no nome do domínio, muitas vezes vinculados a *links* sobre notícias políticas, petições públicas e coalizões populares em oposição aos respectivos governos (MARCZAK et al., 2018). Este *modus operandi* do Pegasus faz uso da engenharia social para induzir o alvo a clicar em *links* que se apresentam como informações de interesse público e com senso de urgência elevado, mas que acabam levando-o a comprometer a segurança e a

impenetrabilidade de seu dispositivo, sem perceber o processo de manipulação no qual está envolvido.

Como consequência desse uso indiscriminado, foram relatados inúmeros casos de violação da privacidade cibernética e da liberdade de expressão por jornalistas e opositores do governo alvos do Pegasus. No México, em 2017, cerca de 25 casos de alvos confirmados com evidências forenses de infecção por Pegasus foram identificados, incluindo advogados, jornalistas, ativistas pelos direitos humanos, políticos da oposição, críticos à corrupção e até mesmo membros de uma investigação internacional da Comissão Interamericana de Direitos Humanos em operação à época. No mesmo ano, a denúncia ganhou uma enorme visibilidade e inspirou a campanha *#GobiernoEspía*, que se tornou um símbolo de mobilização contra o uso de tecnologias de vigilância que intimidam e cerceiam o debate crítico pelo governo mexicano (MARCZAK et al., 2018).

Outro caso emblemático que denunciou o uso arbitrário do software foi do ativista Ahmed Mansoor, nos Emirados Árabes Unidos (EAU) em 2016. Mansoor é um ativista pelos direitos humanos e crítico do governo emiradense, conhecido por denunciar os abusos e a repressão dos EAU contra opositores políticos e jornalistas em suas redes sociais. Ao receber em seu celular, via mensagens de texto, *links* que prometiam supostas denúncias de tortura em prisões nacionais, o ativista desconfiou e encaminhou as mensagens ao Citizen Lab. Após investigar as mensagens encaminhadas, os pesquisadores revelaram um conjunto sofisticado de *exploits* de dia zero - comandos que se aproveitam da falha de um software para fins maliciosos, como instalação de malware ou roubo de dados - que permitiram o desbloqueio remoto do celular e o controle total do dispositivo. Essa foi a primeira vez que o Pegasus foi identificado publicamente, o que expôs mundialmente a colaboração entre a NSO e o governo dos EAU para monitorar e reprimir ativistas no país (MARCZAK et al., 2018). Apesar das denúncias, Mansoor continuou sendo perseguido e foi preso em 2018 por “utilizar as redes sociais para publicar informações falsas e prejudicar a reputação do Estado” (AMNESTY INTERNATIONAL, 2018). Além dele, a Anistia Internacional também revelou ao Citizen Lab que um funcionário e ativista saudita baseado no estrangeiro também foi alvo do Pegasus no mesmo ano, o que demonstra expansão significativa do software em alvos na região do Golfo Pérsico.

Assim, é possível analisar a indústria tecno-militar de Israel a partir do caso Pegasus com base nos pilares erguidos pelo militarismo, pela privatização e pela internacionalização deste mercado. Em primeiro lugar, é nítida a influência do setor de defesa militar israelense na indústria high-tech, fato que foi aprofundado na seção anterior desta pesquisa e é comprovado

no caso Pegasus, uma vez que os fundadores do NSO Group, assim como de diversas outras empresas e *startups* de tecnologia israelense, foram agentes das IDF e especificamente da Unidade 8200. Essa relação orgânica revela o desenvolvimento, produção e venda não apenas de um software inovador, mas sim de uma concreta arma de vigilância global que coleta informações críticas e privadas de alvos considerados de interesse estratégico, como líderes políticos, militares ou agentes de segurança, além de representações de ameaça política, como opositores ao governo, jornalistas e ativistas. Muito além de uma ferramenta digital, o Pegasus representa a evolução do setor militar israelense, que hoje ultrapassa o setor bélico e desenvolve inúmeras técnicas, estratégias e tecnologias multifacetadas para garantir maior vantagem estratégica possível frente a seus aliados e adversários.

Além disso, é também importante pontuar a questão da privatização e da mercantilização da segurança em Israel. Ao passo que empresas privadas se tornam fornecedoras desta tecnologia avançada, com uma porcentagem de lucro significativo e muitas vezes sem medidas de transparência e *accountability* efetivas sobre os clientes finais, o Estado estabelece uma postura de passividade a esse processo, no caso de Israel até incentivando os investimentos do setor privado na indústria de defesa nacional (RUBIN, 2017). Essa dinâmica levanta questões sobre as razões pelas quais o Estado cederia elementos de sua própria soberania, como o setor de segurança, a entidades privadas, ao que Shir Hever (2017) defende que, no caso de Israel, ocorre porque estas mesmas entidades continuam integradas ao ecossistema estatal a benefício do Estado, a exemplo do Programa Magnet (BREZNITZ, 2007). No caso da NSO Group, esse benefício é estendido ao Estado pela empresa ao disponibilizar o uso de sua expertise tecnológica, resultando em uma relação simbiótica entre Estado e setor privado. Assim, essa ideia de "terceirização" - ainda que não integral - do papel do Estado na segurança e na indústria de defesa não implica necessariamente na perda da soberania estatal para a privatização, mas sim na ampliação da sua produção tecnológica e sua consequente capacidade de exportação.

Nesse sentido, por fim, outra base de sustentação que mantém atuante e produtiva a indústria tecnológica de defesa de Israel é sua faceta transnacional. Ao longo das últimas três décadas, o país se consolidou como um polo global de desenvolvimento, produção e exportação de tecnologias de segurança e ciberinteligência, o que resultou em parcerias estratégicas e alianças com governos e empresas privadas em diversos territórios. Nesse contexto, a atuação comprovada do Pegasus em pelo menos 45 países e em quase todos os continentes é símbolo prático desse processo, reforçando a dependência global do mercado tecnológico israelense e levantando dúvidas sobre marcos regulatórios e éticos de um

comércio securitário transnacional em expansão. Além disso, também joga luz na discussão da segurança internacional no meio cibernético, uma vez que pode ser usado para suscitar questões sobre soberania digital, violação de direitos humanos e securitização.

Portanto, o caso Pegasus revela que a vigilância digital ultrapassa fronteiras transnacionais e expõe as fragilidades do controle democrático sobre as tecnologias de vigilância. Em meio ao crescimento mundial de regimes autoritários, a repressão política e social também é transferida para o meio digital, e um produto que teoricamente deveria ser voltado contra o crime organizado é capturado por governos e agências de segurança para uso político doméstico e transnacional. Como afirma Kai Biermann (2024), o Pegasus representa hoje o principal paradigma sobre os perigos do *surveillance* na sociedade moderna e suas implicações para a democracia, o direito à privacidade e os direitos civis. A análise desse ecossistema transnacional formado pela indústria tecnológica de defesa israelense permite compreender sua expansão do espaço doméstico para dinâmicas globais de poder e controle, no qual a segurança se torna instrumento de vigilância política. Assim, não se trata de um caso isolado, mas sim uma expressão concreta de uma tecnologia que ultrapassa fronteiras e desafia o estudo da segurança internacional.

2.3 Do laboratório palestino à exportação

A presente seção propõe expor como o aparato securitário tecnológico israelense, que hoje alimenta uma indústria internacional, se baseia em um produto historicamente colonial, desenvolvido, aplicado e aperfeiçoado no território palestino. Nesse sentido, será abordado como o spyware Pegasus é exemplo prático de uma continuação digital do modelo de governança securitária colonial, que transformou a região ocupada na Palestina em um laboratório para testagem de tecnologias desenvolvidas a partir de investimentos estatais e privados, conforme abordado nas seções anteriores. Assim, busca-se compreender como tecnologias concebidas para controlar a população palestina e reafirmar práticas de dominação passaram a integrar o mercado global de segurança, transformando métodos coloniais em produtos mercadológicos de exportação.

Em primeiro lugar, é preciso compreender que o território palestino ocupado pelas forças israelenses foi transformado em um verdadeiro campo de testes, no qual tecnologias militares e cibernéticas de segurança são refinadas e aperfeiçoadas, para posteriormente serem convertidas em mercadoria para exportação. De acordo com Jeff Halper (2015), Israel não produz apenas armas, mas também táticas, doutrinas e tecnologias de segurança baseadas na

gestão e contenção de populações, desenvolvidas no território palestino. Nesse sentido, a ocupação israelense não se limita ao domínio territorial, mas também ocorre a partir de um regime permanente de vigilância sustentado por práticas de monitoramento, repressão e experimentação, através do uso de ferramentas como reconhecimento facial, drones de identificação e *checkpoints* que funcionam como postos de controle fronteiriço. Assim, a Palestina se tornou um laboratório militar e cibernético de Israel, onde métodos de repressão e vigilância contínua aplicados à população civil são testados e refinados diariamente, aprimorando a ocupação israelense atual em um processo tecnológico e sistemático de gestão populacional.

Nesse contexo, é importante notar como o repetido processo de experimentação das tecnologias de defesa no território palestino é legitimado no âmbito mercadológico. Ao serem empregadas em operações militares ou ofensivas de segurança na região, esses equipamentos e ferramentas recebem o selo de "*combat proven*", ou seja, uma certificação de que foram testados em combate. Esse processo impulsiona a legitimidade técnica dos produtos perante o mercado de segurança, fazendo com que seu valor de mercado aumente e o torne mais competitivo. Dessa forma, como observa Halper (2015), a violência cotidiana contra essa população é instrumentalizada para aprimorar tecnologias de controle e inovação securitária sem qualquer consideração com a preservação dos direitos individuais daqueles cidadãos, desumanizando-os e os transformando em objetos de estudo de um verdadeiro laboratório que combina esforços militares e valores coloniais voltados ao neoliberalismo.

Assim, conforme argumenta Zureik (2020), a associação entre colonialismo e neoliberalismo resulta nos motores do complexo tecno-militar israelense. Ao passo que Rubin (2017) e Breznitz (2007) veem o futuro do setor de segurança israelense baseado na privatização, conforme visto na seção 2.1 desta pesquisa, Zureik dá um passo atrás e mostra que esse futuro é indissociável da ocupação. Enquanto o colonialismo de assentamento perpetrado por Israel na Palestina fornece o campo material e simbólico de testes, o sistema neoliberal alimentado pelo mercado tecnológico israelense converte essa experiência em recurso econômico lucrativo e vantagem competitiva. Dessa forma, este modelo híbrido de dominação favorece a monetização da experiência colonial por empresas privadas de segurança e tecnologia, além de abrir espaço para a coleta involuntária de dados, controle biopolítico daquela população e operação de ferramentas de engenharia social. O resultado é um complexo tecno-militar autossustentável, no qual a ocupação gera inovação e lucro, que por sua vez financiam novas formas de ocupação colonial, dessa vez tecnológica e contemporânea através da vigilância digital.

Essa lógica é fortalecida principalmente após os anos 1990, com o crescimento da indústria *high tech* de defesa em Israel e a proliferação das *startups* no país, conforme aprofundado anteriormente no presente estudo. Nesse contexto, Huberman (2020) estabelece uma "colonização neoliberal" em Jerusalém após os Acordos de Oslo, onde o discurso de desenvolvimento é utilizado como estratégia de pacificação e consolidação territorial em um modelo que políticas de segurança, infraestrutura e inovação tecnológica passam a ser inseridas como ferramentas de controle social em uma lógica de mercado, normalizando a violência em nome do progresso econômico. Assim, essa colonização neoliberal é inserida de forma estrutural nos projetos de urbanismo, infraestrutura, políticas públicas e habitações na região, através de práticas de pacificação do Estado israelense e de atores privados que utilizam mecanismos de segurança, vigilância, controle de mobilidade e segregação espacial para manter a ordem local e conter qualquer movimento de resistência ou insurgência.

A partir disso, é possível compreender essa colonialidade também sob um prisma cibernético, no qual a vigilância digital se torna um mecanismo colonial contemporâneo e parte de uma estrutura neoliberal. A digitalização da ocupação israelense, especialmente em Gaza, representa uma intersecção entre tecnologia, poder e colonialidade na qual se encontram dinâmicas características da globalização neoliberal - nos âmbitos econômicos e tecnológicos - e da colonização israelense, cujas quais são evidentemente contraditórias e, por isso, necessitam de processos contínuos de renovação por parte de Israel, o que garante mais uma vez a sustentabilidade de uma estrutura essencialmente insustentável (GOMES, 2018). Assim, a ocupação digital é responsável por transformar os territórios palestinos em locais extremamente monitorados e controlados em um esforço de manutenção do espaço através da militarização permanente e utilização de sistemas altamente tecnológicos de segurança e cibersegurança. Esse modelo não apenas beneficia e promove os interesses da política local israelense, mas também favorece a inserção do país no mercado global de segurança de alta tecnologia, possibilitando a replicação da lógica colonial em questão a níveis transnacionais (HALPER, 2015).

Tal lógica também se manifesta como ferramenta de manutenção daquilo que Mbembe (2003) define como necropolítica, ou seja, o poder decisório sobre quem deve ser controlado, vigiado e morto. O controle da vida palestina, nesse caso, assume uma forma de racionalidade cibernética e espacializada através do controle, transformando a tecnologia em instrumento de opressão e soberania. Nesse sentido, a população civil daquele território se torna parte de uma infraestrutura de guerra, elementos ativos de um regime de governança securitária que lucra com a precarização (GORDON; PERUGINI, 2020) e com a "classificação de vigilância"

(LYON, 2011), cujo modelo é gradualmente transposto para a esfera internacional, moldando uma governança securitária global, com raízes no colonialismo e no neoliberalismo.

Como afirma Halper (2015), a estrutura deste complexo militar securitário global articula Estados, empresas privadas, universidades e think tanks em um sistema que mercantiliza o setor de segurança internacional nos moldes israelenses de vigilância e controle. Por sua vez, Antony Lowenstein (2023) revela que esse processo alimenta um modelo econômico de governança que expõe o laboratório palestino como uma vitrine comercial de desenvolvimento, testagem e legitimação de tecnologias de vigilância e repressão com a finalidade de serem exportadas e comercializadas globalmente. Nesse sentido, produtos tecnológicos testados sob ocupação são aperfeiçoados sob condições reais de conflito e policiamento e vendidos ao exterior em um modelo de segurança privatizada e globalizada, da qual quem pagar mais garante o acesso.

Assim, é possível afirmar que o *know-how* militar e a vigilância perpetrada pela ocupação israelense, aprimorados ao longo de décadas de monitoramento da população palestina, foram transferidos e comercializados pelo setor privado, que por sua vez recebe apoio institucional e econômico do Estado de Israel. Com isso, foi possível desenvolver produtos de defesa, especialmente no setor de cibersegurança, como o software de espionagem Pegasus produzido pela NSO Group e exportado globalmente a pelo menos 45 países (MARCZAK et. al. 2018). Essa transferência do *know-how* e das tecnologias de vigilância de uma lógica colonial para uma lógica mercadológica internacional, revela não apenas a privatização do setor de segurança estatal, mas também a consolidação de um modelo de governança securitária transnacional. O spyware Pegasus se revela, assim, como uma continuação digital desse modelo de segurança com raízes coloniais, reproduzindo a lógica de vigilância em escala transnacional, normalizado sob o discurso da segurança.

A dissuasão no ciberespaço, como pontua Nye (2017), reforça essa tendência, com a premissa de que a balança de poder internacional também é manipulada através da tecnologia, uma vez que os próprios Estados instrumentalizam, silenciosamente, essa ferramenta em prol de seus interesses próprios. A projeção internacional dessa estratégia, portanto, permite que "atores estatais e não estatais influenciem outros ao penetrar seus sistemas de informação." (NYE, 2017, p. 43), como é o caso do Pegasus. Dessa forma, como defende Halper (2015), a área da segurança internacional foi transformada em um sistema de pacificação permanente, onde o objetivo do Estado não se resume em derrotar um inimigo, mas sim administrar, vigiar e conter populações que podem vir a se tornar inimigas.

Portanto, conforme o exposto, a experiência israelense evidencia como a ocupação e a vigilância da população palestina foram convertidas em expertise técnica e mercadoria securitária, transformando práticas de dominação colonial em ativos do neoliberalismo. Nesse contexto, o setor de tecnologia e cibersegurança em Israel expressa essa dinâmica de forma clara através do Pegasus, um produto factual desse processo, aprimorado pelo sistema de ocupação e vigilância israelense implantado na Palestina. A continuidade desse modelo no meio digital intensifica a sua lógica de uso como ferramenta de dominação, aliada a uma faceta transnacional de governança securitária onde a segurança é transformada em *commodity*. No próximo capítulo, analisaremos como esse modelo pode ser capturado por atores internacionais e legitimado em nome da segurança.

3. QUANDO A TEORIA ENCONTRA A REALIDADE: O CASO PEGASUS COMO EXPRESSÃO DA RECONFIGURAÇÃO SECURITÁRIA INTERNACIONAL

O presente capítulo focará em vincular o debate sobre Segurança Internacional ao processo de securitização dos setores da vigilância e da cibersegurança observado no contexto de Israel, que tende a ser replicado no cenário internacional. Com base no estudo do caso israelense feito até aqui, foi possível notar que o epicentro da produção e desenvolvimento de tecnologias de vigilância e segurança articulou interesses estatais e privados em uma lógica historicamente colonial de mercantilização desses produtos. Nesse sentido, o software Pegasus foi utilizado como objeto empírico de análise em conjunto com o contexto de produção securitária de Israel, e o que se pretende aqui é demonstrar, a partir das contribuições oferecidas pela Escola de Copenhague, pelos Estudos Críticos de Segurança e pelos autores críticos que articulam temas vinculados à tecnopolítica e cibersegurança, como a securitização da tecnologia redefine o debate da Segurança Internacional.

Em primeiro lugar, é importante retomar a análise feita no início desta pesquisa sobre os estudos da Escola de Copenhagen (BUZAN, 1998), para que possamos vinculá-la com o caso prático executado por Israel. Ao romper com o paradigma exclusivamente militarista sobre a segurança internacional, os autores desta Escola abrem margem para o debate do tema em diferentes esferas societárias, reinterpretando ameaças como uma construção social feita por atores securitizantes através de atos discursivos, de forma a legitimar assim a adoção de medidas excepcionais e autoritárias. Essa lógica é fundamental para compreender como Israel, ao longo das décadas, conseguiu securitizar a tecnologia e o meio digital sob o discurso de proteção nacional e prevenção ao terrorismo, narrativa que justifica e legitimiza o uso de tecnologias invasivas e de vigilância, como o Pegasus. Como afirma Loewenstein (2023), após os ataques de 7 de outubro, Israel adotou a mesma lógica dos Estado Unidos após os ataques de 11 de setembro, edificando uma narrativa de combate ao terror que legitima e justifica a adoção de medidas extremas que violam liberdades individuais em prol da segurança nacional. Assim, ao afirmar que o Pegasus é licenciado a agências governamentais e policiais para investigar e prevenir a ocorrência do crime organizado e do terrorismo (MARCZAK et. al., 2018), o papel securitizante do discurso na legitimação dessas práticas se faz evidente e comprova o processo de securitização dos recursos tecnológicos em meio a ameaças modernas e transnacionais.

Nesse sentido, é possível afirmar que *softwares* como o Pegasus, que atuam no processo de securitização do meio digital, legitimam medidas extremas e podem se tornar

instrumentos nefastos ao serem vinculados a regimes autoritários. Retóricas que se alinham à "guerra ao terror" e ao combate ao crime organizado funcionam assim como justificativa para o uso de ferramentas de vigilância que podem se transformar em instrumentos de repressão política e controle social. Nesse cenário, Mudde (2019) identifica a ascensão da quarta onda da extrema direita global no século XXI como um fenômeno que contribuiu para a legitimação e normalização do autoritarismo político e estatal que perpetuam esse discurso de medo e segurança por meios digitais e *mainstream* em escala transnacional. Em complemento a isso, esse contexto político promove inclusive regimes baseados no tecno-autoritarismo, onde o poder é instrumentalizado pelo controle do terror e pela construção discursiva da ameaça, e cria um ciclo de insegurança que é capturado e continuado para legitimar tecnologias de vigilância e concentração de poder (PERON, MAGALHÃES E CAETANO, 2025). Dessa forma, o Pegasus e outras tecnologias de vigilância revelam a convergência entre o processo de securitização digital e o tecno-autoritarismo, na qual a tecnologia se torna essencialmente uma ferramenta de dominação política e de reprodução de práticas autoritárias.

Nesse contexto, também se faz pertinente a retomada da análise acerca dos Estudos Críticos de Segurança, que defendem a emancipação do indivíduo perante as estruturas opressoras estatais (BOOTH, 1991). O caso do Pegasus ilustra a inversão dessa lógica, uma vez que a utilização desta tecnologia não produz segurança social e tampouco promove a emancipação do indivíduo, mas sim restringe liberdades pessoais ao monitorar dados pessoais e reproduz estruturas de poder opressoras ao utilizar essas informações contra o próprio indivíduo. Conforme revelado pelo *Citizen Lab* (MARCZAK et. al., 2018) e elencado ao longo desta pesquisa, a ferramenta foi empregada contra jornalistas, advogados, ativistas e opositores políticos em diversos países como Emirados Árabes Unidos, México e Arábia Saudita, revelando a instrumentalização da tecnologia por regimes democráticos e autoritários para monitorar e silenciar vozes críticas da sociedade civil naqueles países. Esses episódios revelam as contradições centrais dessa tecnologia, que vem sendo utilizada de forma a cercear a liberdade de expressão e o direito à privacidade dos alvos, substituindo a função emancipatória da segurança por mais uma forma de opressão do Estado.

Tendo em vista essa conjuntura, é reforçada a premissa de que a tecnologia não é neutra e reproduz relações de poder e interesses políticos de uma classe dominante. Como defendem MacKenzie e Wajcman (1999), novas tecnologias estão intrinsecamente conectadas ao contexto político e institucional ao qual elas são produzidas, sendo portanto produtos históricos e sociais que refletem estruturas de controle. Nesse sentido, toda tecnologia

incorpora uma política (WINNER, 1999), e no caso israelense, o Pegasus expressa uma política autoritária de raízes coloniais, onde a tecnologia é mobilizada para manter o controle de populações oprimidas mas, também, reflete a continuação desse regime de opressão colonial com a produção e desenvolvimento tecnológicos em território ocupado. Como observa Mumford (1967), regimes autoritários tendem a produzir tecnologias autoritárias, que, assim como o aparato securitário israelense, são moldadas por lógicas de comando, hierarquia e eficiência. O produto dessa racionalidade tecnológica (MARCUSE, 1964) transforma a eficiência técnica e o desenvolvimento tecnológico em ferramentas de opressão e vigilância que garantem o exercício do poder. Assim, a tecnologia se torna mais um instrumento de dominação permeado por um discurso de eficiência técnica e de lógica securitária.

Dessa forma, assim como a tecnologia incorpora políticas e reproduz contextos institucionais, ela também possibilita a continuação de padrões de ameaça baseados em uma lógica embranquecida e ocidental, que remonta a um modelo estruturalmente racista e colonial (BENJAMIN, 2019). Crawford (2021) defende essa análise através do conceito de colonialismo de dados, onde a população marginalizada é transformada em matéria de estudo informacional e explorada em benefício do desenvolvimento tecnológico e militar, sendo a Palestina o maior exemplo deste processo. Assim, o Pegasus também atua como uma ferramenta do colonialismo digital ao ser produto da coleta, classificação e mercantilização da vigilância do comportamento palestino, transformado em uma política econômica de segurança. É nesse espaço que o trabalho de Zuboff (2019) encontra terreno fértil para sistematizar o conceito de capitalismo de vigilância, onde dados comportamentais são capturados e transformados em lucro, transformando a vigilância em uma mercadoria global.

Assim, a cooperação estrutural entre agentes públicos e privados na consolidação e configuração desse novo modelo de segurança internacional é estabelecida. Atores do setor privado, como a NSO Group, penetram o aparato estatal e passam a ocupar funções essencialmente atribuídas ao Estado, redefinindo a formulação e execução de políticas de segurança nacional como em uma verdadeira República Neoliberal (Vauchez; France, 2020). Dessa forma, a segurança deixa de ser monopólio estatal e é transformada em um produto de economia política, um *assemblage* securitário transnacional de práticas, discursos e atores que produzem, legitimam e circulam globalmente modelos de segurança (ABRAHAMSEM; WILLIAMS, 2007). Israel e o caso Pegasus, especialmente, são exemplos práticos paradigmáticos desse fenômeno, onde a lógica neoliberal, o *know-how* militar e o capital

tecnológico convergem na produção e exportação de modelos de vigilância e controle com fins políticos e econômicos.

Portanto, a presente análise traz à tona um modelo de segurança internacional contemporâneo moldado por lógicas neoliberais, que transformam a segurança e a vigilância em produtos econômicos lucrativos. O caso israelense demonstra de forma prática um aparato tecno-militar construído ao longo de décadas com raízes coloniais ainda estimulada atualmente, projetado para o abastecimento de um mercado global e legitimado pelo discurso de segurança nacional. A atuação de empresas como a NSO Group e a utilização do Pegasus nesse contexto são símbolos de um regime de poder que une lógica colonial, mercado neoliberal e racionalidade securitária em uma dinâmica que redefine e reconfigura o próprio conceito de segurança internacional, onde outros atores não estatais se tornam influentes e o poder não se faz necessariamente pela coerção, mas sim pela tecnologia.

CONCLUSÃO

Diante do exposto, o que se evidencia é um redirecionamento estratégico das ferramentas de segurança internacional para o meio digital e cibernético, sustentado pelo setor privado e estimulado pela lógica neoliberal. Nesse ínterim, o processo de securitização da vigilância digital pelo mercado de segurança e tecnologia de Israel, em cooperação com o Estado, torna-se evidente, redefinindo as dinâmicas e o debate acerca da segurança internacional contemporânea. Assim, a presente pesquisa buscou compreender, a partir do estudo de caso do software Pegasus, os efeitos deste processo de securitização nos estudos de área de segurança internacional e suas implicações políticas em contexto global.

Nesse contexto, em um primeiro momento, o estudo acerca dos fundamentos teóricos da segurança e da tecnologia na área de Relações Internacionais foram de suma importância para interpretar o contexto atual da agenda securitária internacional. Com isso, a partir da Escola de Copenhagen e dos Estudos Críticos de Segurança, foi possível ampliar o conceito tradicional de segurança centrado no militarismo e com foco na atuação do Estado, compreendendo assim a incorporação de atores privados e estratégias discursivas na construção social da ameaça. Essa base teórica, suplementada por abordagens mais aprofundadas e específicas, permitiu assimilar a instrumentalização política do meio digital, evidenciando como as tecnologias de informação e vigilância se tornaram ferramentas de poder e controle nas dinâmicas internacionais contemporâneas. A partir dessas abordagens, foi possível compreender como o meio digital se tornou um novo campo de securitização, no qual a vigilância e o controle tecnológico passam a ser tratados como questões de segurança nacional e global.

Em seguida, concentrando a análise na indústria tecno-militar de Israel, foi possível compreender como o país desenvolveu esse setor ao longo das décadas e se transformou em um polo global de inovação tecnológica securitária. A expertise militar israelense, adquirida ao longo dos anos durante a ocupação palestina, foi incorporada pelo setor privado e vendida como produto em um modelo transnacional de segurança, consolidando um ecossistema de defesa que se autossustenta. Nesse sentido, a escolha por realizar um estudo de caso do software Pegasus se fez para exemplificar, de forma concreta, essa dinâmica de desenvolvimento da tecnologia e exportação para o estrangeiro, além de revelar a transposição de práticas de controle e vigilância com origens coloniais.

Por fim, em um esforço de articulação entre os estudos de segurança e a securitização do meio tecnológico, tomando o Pegasus como expressão factual dessa lógica no presente

estudo, a análise evidenciou a transformação da tecnologia e da vigilância em instrumento político de poder e lucro. A segurança no campo cibernético, nesse sentido, permeada por tecnologias que estão longe de serem neutras, se vê moldada por interesses de atores privados e políticos que, no caso estudado, possui raízes históricas coloniais e perpetuam desigualdades estruturais. Assim, ao ser comercializada no mercado securitário global em uma lógica econômica neoliberal, consolida um modelo de segurança transnacional em que a tecnologia se torna um novo vetor de dominação.

Dessa forma, a análise permitiu observar que a securitização tecnológica ultrapassa o campo militar e se consolida como um novo eixo de poder transnacional, sustentado por uma lógica neoliberal e colonial de vigilância e controle social. Apesar das limitações presentes na pesquisa, como a dificuldade no acesso a dados sigilosos e documentos oficiais da empresa, além da escassez de literatura brasileira acerca do tema, o presente estudo demonstrou como o Pegasus se tornou um paradigma do capitalismo de vigilância, legitimando e normalizando o monitoramento digital em regimes autoritários e democráticos em nome da segurança nacional. Assim, o estudo se faz essencial para compreender o avanço dos estudos de segurança internacional no século XX, seus limites éticos e políticos e sua relevância nas Relações Internacionais, em um mundo cada vez mais globalizado e tecnológico.

Em suma, este trabalho buscou compreender o processo de securitização tecnológica produzido por Israel, através de um estudo de caso do software Pegasus, que foi difundido globalmente por diversos países. A partir dessa análise, foi possível perceber uma redefinição das dinâmicas de segurança internacional contemporânea, que pode sustentar uma investigação mais aprofundada sobre um novo modelo de governança securitária transnacional, influenciada pelo setor privado e pelo meio digital. Portanto, o presente estudo visa contribuir para o campo de estudos sobre paz, defesa e segurança internacional, frente um fenômeno global de inovação tecnológica testemunhado na contemporaneidade.

BIBLIOGRAFIA

AMNESTY INTERNATIONAL. UAE: Activist Ahmed Mansoor sentenced to 10 years in prison for social media posts. Londres: **Amnesty International**, 31 mai. 2018. Disponível em: https://www.amnesty.org/en/latest/news/2018/05/uae-activist-ahmed-mansoor-sentenced-to-10-years-in-prison-for-social-media-posts/. Acesso em: 3 out. 2025.

BENJAMIN, Ruha. **Race after technology: abolitionist tools for the new Jim code.** Cambridge: Polity Press, 2019.

BIERMANN, Kai. Pegasus: the unbounded surveillance industry in the service of the authoritarian. In: FRANKENBERG, Günter; HEITMEYER, Wilhelm (orgs.). **Drivers of Authoritarianism: Paths and Developments at the Beginning of the 21st Century**. Cheltenham: Edward Elgar Publishing, 2024.

BOOTH, Ken. Strategy and emancipation. **Review of International Studies**, Cambridge, v. 17, n. 4, 1991.

BOOTH, Ken. **Theory of world security**. Cambridge: Cambridge University Press, 2000.

BREZNITZ, Dan. **Innovation and the State: Political Choice and Strategies for Growth in Israel, Taiwan, and Ireland**. New Haven: Yale University Press, 2007.

BUZAN, Barry; WÆVER, Ole; DE WILDE, Jaap. **Security: A New Framework for Analysis**. Boulder: Lynne Rienner Publishers, 1998.

CARR, Edward Hallett. **Vinte anos de crise: 1919-1939: uma introdução ao estudo das relações internacionais.** Tradução de Luiz Alberto Figueiredo Machado. Brasília: Editora Universidade de Brasília; São Paulo: Imprensa Oficial do Estado, 2001.

COHEN, Avner. **Israel and the Bomb.** New York: Columbia University Press, 1998.

CRAWFORD, Kate. **Atlas of AI: power, politics, and the planetary costs of artificial intelligence**. New Haven: Yale University Press, 2021.

DEIBERT, Ronald. The road to digital unfreedom: three painful truths about social media. In: DIAMOND, Larry; PLATTNER, Marc (org.). **Authoritarianism goes global: the challenge to democracy.** Baltimore: Johns Hopkins University Press, 2015.

GALTUNG, Johan. **Violence, peace, and peace research**. Journal of Peace Research, v. 6, n. 3, 1969.

GOMES, Julia Tibiriçá Diegues. **Dimensões cibernéticas de colonialidade, controle e resistência na Palestina ocupada.** 2018. Dissertação (Mestrado em Ciência Política) - Faculdade de Filosofia, Letras e Ciências Humanas, University of São Paulo, São Paulo, 2018.

GORDON, Neve; PERUGINI, Nicola. **Human Shields: A History of People in the Line of Fire**. 1st ed., University of California Press, 2020.

HALPER, Jeff. **War Against the People: Israel, the Palestinians and Global Pacification.** London: Pluto Press, 2015.

HEVER, Shir. **The Privatization of Israeli Security**. London: Pluto Press, 2017.

HUBERMAN, Bruno. **A colonização neoliberal de Jerusalém pós-Oslo: desenvolvimento, pacificação e resistência em Palestina/Israel**. 2020. 356 f. Tese (Doutorado em Relações Internacionais) – Programa de Pós-Graduação San Tiago Dantas (UNESP – UNICAMP – PUC-SP), São Paulo, 2020.

IVC RESEARCH CENTER Ltd. **The Israeli Cyber Technology Cluster: The Cyber Cluster Explained.** Tel Aviv: IVC Research Center, Jan. 2016. Disponível em: https://www.ivc-online.com/Portals/0/RC/The%20Israeli%20Cyber%20Technology%20Cluster_final.pdf. Acesso em: 3 out. 2025.

KHALIDI, Walid (org.). **All That Remains: The Palestinian Villages Occupied and Depopulated by Israel in 1948**. Washington, D.C.: Institute for Palestine Studies, 1992.

LEE, Aileen. **Welcome to the Unicorn Club: Learning from Billion-Dollar Startups**. TechCrunch, 2 dez. 2013.

LOWENSTEIN, Antony. **The Palestine Laboratory: How Israel exports the technology of occupation around the world**, Verso Books, 2023.

LYON, David. "Identification, colonialism and control: surveillant sorting in Israel/Palestine" in: **Surveillance and Control in Israel/Palestine: Population, Territory and Power.** London: Routledge. 2011.

MACKENZIE, Donald; WAJCMAN, Judy (org.). **The social shaping of technology.** 2. ed. Buckingham: Open University Press, 1999.

MARCUSE, Herbert. Algumas implicações sociais da tecnologia moderna. In: MARCUSE, Herbert. **Tecnologia, guerra e fascismo**. Tradução de Luiz Sérgio Henriques. Rio de Janeiro: Paz e Terra, 1998.

MARCZAK, Bill; SCOTT-RAILTON, John; MCKUNE, Sarah; RAZZAK, Bahr Abdul; DEIBERT, Ron. **Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries**. Citizen Lab Research Report No. 113, University of Toronto, September 2018.

MBEMBE, Achille. Necropolitics, **Public Culture** 15 (1) 11-40, 2003.

MEARSHEIMER, John J. **The Tragedy of Great Power Politics**. New York: W. W. Norton & Company, 2001.

MEARSHEIMER, John J.; WALT, Stephen M. **The Israel Lobby and U.S. Foreign Policy**. New York: Farrar, Straus and Giroux, 2007.

MORGENTHAU, Hans J. **A política entre as nações: a luta pela guerra e pela paz.** Brasília: Editora Universidade de Brasília/ Instituto de Pesquisa de Relações Internacionais; São Paulo: Imprensa Oficial do Estado de São Paulo, 2003.

MORRIS, Benny. **Righteous Victims: A History of the Zionist-Arab Conflict, 1881–1999**. New York: Vintage, 2001.

MUMFORD, Lewis. Authoritarian and democratic techniques. **Technology and Culture**, v. 5, n. 1, p. 1–8, winter 1964.

Nye, Joseph. **Soft power: as origens e o progresso político de um conceito**. Palgrave Commun 3 , 17008 (2017).

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Assembleia Geral. **Resolução 181 (II). Futuro Governo da Palestina.** Nova Iorque: ONU, 29 nov. 1947. Disponível em: https://undocs.org/en/A/RES/181(II). Acesso em: 20 ago. 2025.

PAPPÉ, Ilan. **The Ethnic Cleansing of Palestine**. Oxford: Oneworld, 2006.

PERON, Alcides Eduardo dos Reis; MAGALHÃES, David Almstadter Mattar de; CAETANO, Gabriel Fernandes. Beyond digital repression: techno-authoritarianism in radical right governments. **Cogent Social Sciences**, v. 11, n. 1, 2025.

RUBIN, Uzi. **Israel's defence industries: an overview**. Defence Studies, 17(3), 228–241, 2017.

SHLAIM, Avi. **A muralha de ferro: Israel e o mundo árabe.** Trad. Maria Beatriz Penna Vogel. Rio de Janeiro: Fissus Ed., 2004.

STAMPNITZKY, Lisa. **Disciplining terror: how experts invented terrorism".** NY: Cambridge University Press. 2013.

TISHLER, Asher; PINCHAS, Gil. **Challenges of the Israeli Defense Industry in the Global Security Market**. In: HADAD, Sasson; FADLON, Tomer; EVEN, Shmuel (eds.). Challenges of the Israeli Defense Industry in the Global Security Market. Memo 202. Tel Aviv: Institute for National Security Studies (INSS), 2020. p. 35-49. Disponível em: https://www.inss.org.il/wp-content/uploads/2020/08/Memo202_e-35-49.pdf. Acesso em: 30 set. 2025.

UNITED STATES. Congress. Office of Technology Assessment. **Global arms trade: commerce in advanced military technology**. Washington, D.C.: U.S. Government Printing Office, Cap. 5: Israel's defense industry: evolution and prospects, 1991.

VAUCHEZ, Antoine; FRANCE, Pierre. **The Neoliberal Republic: Corporate Lawyers, Statecraft, and the Making of Public-Private France**. Ithaca: Cornell University Press, 2020.

VOHRA, Anchal. **Israel's military-technology complex is one of a kind**. Foreign Policy, 19 dez. 2023. Disponível em: https://foreignpolicy.com/2023/12/19/israels-military-technology-complex-is-one-of-a-kind/. Acesso em: 30 set. 2025.

WINNER, Langdon. Do artifacts have politics? In: MACKEY, Andrew (org.). **Technology and values: essential readings.** Malden: Blackwell Publishing, 1999.

WYN JONES, Richard. “Message in a bottle”? Theory and praxis in Critical Security Studies. **Contemporary Security Policy**, Londres, v. 16, n. 3, 1995.

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

ZUREIK, Elia. **Israel’s Colonial Project in Palestine: Brutal Pursuit.** London: Routledge, 2020.