Da guerra à violência permanente: a imanência autoritária das tecnologias securitárias baseadas em IA

From war to permanent violence: the authoritarian immanence of ai-based security technologies

Rev. Bras. Est. Def. v. 11, n. 2, jul./dez. 2024, p. 277–300
DOI: 10.26792/RBED.v11n2.2024.75411
ISSN 2358-3932

ALCIDES EDUARDO DOS REIS PERON

INTRODUÇÃO

Antes de Jomini e Clausewitz, o sucesso na guerra era principalmente atribuído à bravura dos soldados, com alguma admiração pelos estratagemas dos comandantes. A tecnologia era considerada menos importante, e a guerra era vista como resultado das ações individuais. No entanto, nas obras mais recentes, a estratégia e a busca pela previsibilidade e estabilidade desempenham um papel central na discussão sobre a organização e mobilização para o conflito.

Em ambos os autores, a preparação para a guerra, o conhecimento das táticas e territórios inimigos e a organização das estratégias de combate fazem parte de um processo de racionalização da guerra. Em Jomini, isso se reflete na logística e no suprimento das forças. Em Clausewitz, a guerra é vista como um ato político e lógico, buscando previsibilidade e resiliência, orquestrada por profissionais. A estratégia, descrita por Bousquet (2022) como uma técnica em busca de previsibilidade e estabilidade, é o eixo central na transformação da guerra ao longo do tempo. No entanto, ainda assim, para ambos os autores, a tecnologia é considerada uma mera ferramenta da estratégia, não um fator decisivo que a redefine.

Historiadores modernos têm explorado o papel fundamental da tecnologia na evolução das estratégias de guerra e na transformação da própria guerra. Van Creveld (1991, 321) destaca que a tecnologia desempenha um papel significativo nas mudanças das táticas e estratégias de guerra em diferentes eras, indo além de considerações racionais ou físicas. Keagan (2006,

Alcides Eduardo dos Reis Peron é doutor em Política Científica e Tecnológica pela Unicamp. Realizou estágio pós-doutoral em Sociologia na USP. Professor e Coordenador do curso de Relações Internacionais da Fecap. Orcid.org/0000-0003-4537-2775 E-mail: alcides.peron@fecap.br.

464) examina a relação entre guerra e cultura, revelando como as culturas são sensíveis às influências hostis, incluindo o uso de tecnologias avançadas em conflitos, mesmo que isso vá contra a moral e os códigos de honra tradicionais. Virilio e Lotringer (1984) argumentam que a "inteligência" militar não tem limites em sua produção tecnológica, expandindo-se para diversas áreas sociais, econômicas e urbanas, não se restringindo apenas ao aspecto militar. Autores contemporâneos, como Graham (2016), observam que sistemas de armas e tecnologias de guerra transcendem barreiras temporais e espaciais, influenciando as cidades e criando um "urbanismo militar".

Estas interpretações descrevem como a guerra e a estratégia não estão limitados apenas aos desígnios dos operadores da guerra, mas se estendem e são moldados também por uma ampla rede de atores, sistemas e artefatos relacionados à dinâmica de inovação e produtiva de países. Demonstram ainda como sistemas sociotécnicos influenciam de modo determinante os modos de guerra e as racionalidades estratégicas, e em certa medida, se colocam como protagonistas na complexificação da guerra, e de outros processos sociais.

O papel da tecnologia na guerra se destacou no final da Guerra Fria, com avanços significativos em tecnologias da informação e cibernéticas usadas em contextos militares e na interoperabilidade militar. Isso resultou em um aumento do protagonismo da tecnologia na viabilização de novas estratégias e na expansão do escopo da guerra, o que Gros (2008) chamou de "estouro estratégico" da guerra. A tecnologia, impulsionada por atores privados em colaboração com operadores militares, não apenas afetou a guerra, mas a reconfigurou como um evento mais difuso, amplo e imanente, operando em diversos espaços e sustentando práticas repressivas e violentas. Autores como Bousquet (2022), Der Derian (2009) e Harcourt (2020) exploraram as novas tecnologias cibernéticas e digitais para entender como a guerra está sendo transformada em um evento mais amplo e imanente, estruturado como um aparato para gerenciar a complexidade informacional e normalizado como parte do controle social. Na sua perspectiva, a cibernética e os sistemas digitais autônomos de armas estão provocando reconfigurações profundas, tornando porosas as linhas que dividem guerra e paz, interno e externo, e edificando a guerra como um modelo de governança social.

Assim, este artigo discute como as tecnologias baseadas em IA coroam o movimento da cibernética — de produção de controle e previsibilidade no ambiente na gestão da guerra — ao mesmo tempo em que ultrapassam os limites humanitários nos conflitos, e se espraiam enquanto mecanismo de controle social abusivos em ambientes urbanos. Nesse sentido, mais do que sofisticar os meios de destruição nos conflitos armados, a IA corrobora

com a reconfiguração da guerra enquanto um modelo de controle social, potencialmente reprodutor de violências diretas e indiretas. Inicialmente, nos debruçaremos sobre as noções de construção política da tecnologia (Winner 1986), grandes sistemas sociotécnicos (Hughes 2012) e de cosmotécnicas particulares (Huk 2020), para discutirmos como essa trajetória da cibernética não segue um progresso linear neutro, e que, portanto, esse espraiamento da guerra como mecanismo de controle (contrainsurgência) assume os contornos de um modelo projetado pelos EUA de governo social desde a Revolução nos Assuntos Militares (RAM). Em seguida, analisaremos as características da IA e seus principais riscos securitários, para enfim analisarmos projetos militares e policialescos como aparatos que reforçam o seu potencial autoritário.

CIÊNCIA, TECNOLOGIA E AUTORITARISMO

Marx (2011) critica a visão clássica sobre a neutralidade dos fatores de produção, argumentando que o processo de automação não apenas afeta a eficiência econômica, mas também reconfigura a estrutura social, reduzindo o poder dos trabalhadores em relação ao capital, tornando-os dispensáveis no mercado de trabalho e minando sua influência política:

> [...] A máquina não é apenas o concorrente todo-poderoso, sempre pronto a tornar "supérfluo" o assalariado. [...] Ela se torna a arma mais poderosa para reprimir as revoltas periódicas e as greves dos trabalhadores contra a autocracia do capital. (Marx 2011, 492–7).

Portanto, cai por terra a noção de que a tecnologia seria um artifício gerido e dedicado exclusivamente ao aumento da produtividade, resultado de um progresso técnico linear e neutro. Ela se configuraria como um dos instrumentos de poder na disputa entre capital-trabalho, sendo cravejada de sentidos e efeitos políticos, para além do espectro econômico.

Essa perspectiva "sonambulista" da tecnologia, foi sendo contestada no campo das ciências sociais de modo mais incisivo na década de 1970. Como analisam Velho (2011) e Stokes (2005), no imediato pós-guerra, a perspectiva dominante nos EUA e globalmente era de que a ciência básica serviria como um aporte ao progresso tecnológico; em outras palavras, de que o investimento em ciência necessariamente se traduziria em inovações tecnológicas, suportando o projeto hegemônico dos EUA. Nesse sentido, a ciência e a tecnologia eram percebidas como práticas e produções exclusivas de cientistas ligados a universidades e agências, e, portanto, tratava-se de um conhecimento neutro e desinteressado (politicamente), ou mesmo de um acúmulo neutro de conhecimentos e téc-

nicas, orientadas para o progresso social e econômico. Essa perspectiva reforçava a visão de neutralidade da ciência e da tecnologia em suas dimensões sociais, negando a existência de efeitos pervasivos adversos que não fossem resultado de maus usos. Mais do que isso, reforçava a ideia de uma "tecnociência", em que a ciência seria uma condição *sine qua non* para geração de tecnologia, algo que seria muito criticado posteriormente (Rosenberg 1982).

As crises dos anos 1970 e 1980, como o acidente de Chernobyl, problemas ambientais causados pelo uso de pesticidas, a destruição da guerra do Vietnã, o crescente desemprego fruto da mecanização e da informatização, além de uma série de outros eventos resultado desse progresso técnico, colocaram em xeque a perspectiva inconteste sobre o progresso linear e neutro da tecnociência (Velho 2011). A proliferação de empresas e de agentes que agora atuam na produção tecnocientífica coloca em xeque a exclusividade — e a neutralidade — do cientista como ente produtor de conhecimento. Nesse período, os efeitos negativos da tecnociência passaram a ser interpretados não como resultado de "maus usos", porém como algo relacionado às determinações políticas e sociais de sua construção.

Assim, o Construtivismo Social da Ciência e da Tecnologia (SCOT) emerge em conexão direta com as ideias do construtivismo social do século XX, rejeitando a passividade dos indivíduos na realidade social — entende que estes seriam ao mesmo tempo constituídos e constituidores dos diferentes contextos sociais nos quais estão inseridos. No SCOT, argumenta-se que a produção de conhecimento científico é moldada pela interação com o mundo social, sujeita a influências internas e externas. Além disso, o SCOT descarta a visão de que a tecnologia é uma manifestação linear do conhecimento científico, considerando-a um processo multidirecional moldado por grupos sociais diversos e sua estrutura tecnológica (interesses, valores, objetivos, práticas e perspectivas, desacordos e controvérsias). Em resumo, tanto a ciência quanto a tecnologia são co-construídas socialmente, influenciadas por dinâmicas políticas, processos sociais e disputas múltiplas, como defendido por vários autores, como Bourdieu (2004), Latour e Woogar (1988), e Pinch e Bjiker (2012).

Nesse espectro da co-construção entre tecnologia e sociedade, Winner (1986) pontua que, mais do que grupos sociais, há posições políticas, valores e princípios morais predispostas no processo de construção tecnológica. Não apenas o processo de elaboração da tecnologia está envolto em disputas políticas, mas os artefatos em si carregam essa política imanente em seu desenho. Winner entende que as disputas de cunho político-sociais manifestas no desenho final dos artefatos, são perpetuadas

e reproduzidas em seu uso, promovendo "significativas alterações nos padrões de atividade humana e suas instituições" (Winner 1986, 6). No entanto, ele destaca que, em geral, as decisões humanas durante o desenvolvimento da tecnologia são geralmente mascaradas, dando a impressão de que a tecnologia evolui e opera além do controle humano. Aqui reside o principal elemento de sua análise: padrões de poder e autoridade impressos nos artefatos são frequentemente obliterados da percepção humana e social, o que faz com que a reprodução desses valores e práticas sejam mais eficientes e normalizados.

Em sintonia, Hughes (2012) aponta que é difícil estabelecer uma distinção entre o aspecto tecnológico e o social, uma vez que é desinteligente separar os objetos técnicos dos sistemas complexos que os governam e dos quais dependem. Os sistemas tecnológicos são intrincadas combinações de elementos físicos, empresas, instituições financeiras, regulamentações, políticas, discursos, publicações, recursos naturais e elementos construídos socialmente, todos adaptados para funcionar como sistemas. Portanto, eles seguem diretrizes políticas e estratégicas (Hughes 2012, 45). Eles representam as infraestruturas físicas, discursivas, ideológicas e sociais que possibilitam a circulação de valores e interesses no processo de desenvolvimento tecnológico, culminando em decisões políticas relacionadas aos objetos técnicos. Assim, para compreender as tecnologias e a política que as envolve, é essencial entender como elas se integram nos sistemas tecnológicos, econômicos e nas estruturas políticas que tornam sua existência possível.

É patente, portanto, que os contextos, isto é, tendências, arranjos, valores, formas e imanências políticas em uma sociedade acabam sendo incorporadas e perpetuadas pelos arranjos sociotécnicos nele desenvolvidos. Como apontam Mackenzie e Wajcman (1999, 15), mais do que as relações sociais do mercado influenciam as trajetórias tecnológicas, mas também os contextos políticos, culturais e o próprio Estado protagonizam os processos de desenvolvimento tecnológico. Por esse motivo, as cosmotécnicas — a unificação do cosmos e da moral por meio das atividades técnicas — nunca serão universais, mas sempre particulares, como propõe Huk (2020, 39). Haveria muitas trajetórias tecnológicas possíveis, rumos possíveis, dada a diversidade política e cultural global — porém, arranjos socio-culturais e políticos, dinâmicas e disputas de poder específicos podem aniquilar certas trajetórias. Portanto, pensar a tecnologia como resultado de um único curso racional possível é padecer diante de um aparato instrumentalista que dilui a cosmotécnica particular a uma universal, que não conecta a tecnologia com o social, e com suas potencialidades para possíveis novas cosmopolíticas (Huk 2020).

A GUERRA E A TECNOLOGIA

Até recentemente, os Estudos de Segurança muitas vezes negligenciaram a política da tecnologia. A ênfase estava nos efeitos do uso da tecnologia e como ela facilitava estratégias, mas raramente se explorava como a tecnologia mudava a dinâmica do conflito e afetava além do campo de batalha.

Morgenthau (1964) descrevia um Estado centrado nos EUA que promovia inovações, liderado por uma elite tecnocientífica, adotando um modelo linear-ofertista de tecnociência. Por outro lado, para Waltz (2001), a técnica e a tecnologia eram consideradas apenas componentes cumulativos do poder do Estado, sem investigação sobre os efeitos políticos e sociais da tecnologia além do poder. A década de 1980 trouxe uma visão mais multicêntrica da segurança, mas levou quase duas décadas para que se começasse a compreender melhor o aspecto social e político da tecnologia. Autores como Hansen e Nissembaum (2009), por exemplo, começaram a explorar ameaças cibernéticas e imagens como elementos relacionados à segurança. Foi com os Estudos Críticos de Segurança que a relação entre Ciência, Tecnologia e Sociedade e a política da tecnologia se tornaram mais evidentes nas práticas de segurança.

Estes trabalhos, embora forneçam *insights* valiosos sobre aspectos autoritários nas estratégias de segurança, se concentram principalmente em aplicações específicas de tecnologias alinhadas a um modelo de governança liberal. No entanto, eles não conseguem capturar as dinâmicas políticas subjacentes e seus impactos nos aparatos de guerra e segurança. Para entender o contexto mais amplo em que a guerra se torna um modelo de governança social, é essencial analisar as tendências gerais e os efeitos sociopolíticos das tecnologias, algo que exploraremos mais adiante.

Tais tendências foram mais bem exploradas por autores não necessariamente ligados às Relações Internacionais ou à geopolítica, mas em geral, à filosofia política e à filosofia da tecnologia. Enquanto Virilio (2002) e Bousquet (2022) exploraram como, ao longo do século XX, as tecnologias de guerra foram assimilando o espírito político de certos contextos, Harcourt (2021) tem buscado relatar o modo como certas tecnologias — direcionadas à comando e controle — tem sido a chave para estruturar o modelo da guerra como forma de governo social — frequentemente violento e intrusivo.

Virilio, em seus diversos escritos, descreveu como a guerra, em sua dimensão estética e tecnológica, tem um papel relevante na organização do mundo social, e nesse processo, a velocidade (principalmente das tecnologias digitais) cumpre um papel determinante: de articular e normalizar a

perda da autonomia humana. O pensamento de Virilio se caracteriza enquanto um esforço "epistemo-técnico" para compreender a relação entre a tecnologia, o político e seu efeito sobre o humano. É nesse sentido que o autor nos propõe discutir "instantaneamente a substância e o acidente", ou seja, o efeito da aceleração das novas tecnologias e seu resultado desastroso ao mesmo tempo. A tecnologia e o seu acidente (efeitos deletérios, antevistos ou não) revelam a não linearidade do progresso tecnológico, e sua negligência apenas reforça o desaparecimento da dimensão política inerente à tecnologia (Peron 2019).

A dinâmica das inovações tecnológicas militares ao longo do século XX, assim, pode ser sumarizada como uma busca pelo domínio e supremacia da velocidade (Virilio 2002, 25). Para Virilio, a guerra resume-se na organização e produção para a velocidade, seja ela metabólica (do ritmo produtivo e de avanço dos corpos no campo de batalha e no preparo para a guerra), seja ela tecnológica (a corrida pela produção do melhor armamento, a logística de guerra, a velocidade dos instrumentos e da capacidade de comunicação e decepção no conflito). Nesse sentido, todo o conjunto tecnológico desenvolvido ao longo do século XX, no espectro militar, buscava domar essa velocidade no campo de batalha e além, com isso adquirindo uma superioridade maquínico-bélica sobre os inimigos, na dimensão tática, estratégica e logística.

Nessas três dimensões, a aceleração (criativa, no estágio da concepção, e do desempenho, no estágio da ação) é o eixo central que rege o desenvolvimento das tecnologias bélicas. A aceleração atinge seu ápice com o avanço da cibernética, e seu fortalecimento com o desenvolvimento das tecnologias informacionais, responsáveis pelo incremento da digitalização, e a crescente automatização dos sistemas sociotécnicos.

Isso para Virilio é uma questão significativa, posto que a aceleração produzida pelos "motores informacionais", ao conferir maior automação às máquinas, processos produtivos são intensificados, a logística do cotidiano e da guerra também o são, ao ponto de liberar o ser humano da permanente atenção, ou o controle sobre esses processos. Os motores informacionais conferem uma velocidade às máquinas e processos maior que a da percepção e raciocínio humanos, fazendo com que estes incorram em substanciais perdas perceptivas e de autonomia, e, justamente por isso, Virilio se refere a esse processo como um "assujeitamento cibernético" do humano.

Como também especificado por Bousquet (2022), o projeto da Cibernética, tal como concebido por Wierner, busca o aprimoramento de sistemas computacionais e informacionais capazes de decifrar as dinâmicas de raciocínio e funcionamento do corpo humano. A Cibernética é entendida como o "estudo das mensagens como meios de controle da maquinaria

e da sociedade, do desenvolvimento de máquinas computacionais e outros autômatos, de reflexões sobre psicologia e o sistema nervoso, e uma tentativa de uma nova teoria do método científico" (Wierner 1988, 16). Ela compreende todas as trocas em um sistema (nervoso e sensorial, quando reduzido à escala humana, ou administrativo, computacional e gerencial, quando referente a escalas processuais) enquanto trocas informacionais, e, nesse contexto, permite o desenvolvimento de técnicas e linguagens para a compreensão dos problemas de controle, comunicação e ordem. Portanto, o "assujeitamento cibernético" ocorre na medida em que esse conjunto cibernético assume um protagonismo maior do que a ação humana na produção de comunicação, tornando o humano amplamente submisso e secundário.[1]

O termo Cibernética envolve a ideia de governo e controle no gerenciamento de fluxos de informações do modo mais eficiente possível, atribuindo ordem a um sistema caótico e desordenado. Nessa atribuição de ordem sobre o caos a partir do controle informacional, produz-se controle e estabilidade, e assim, a Cibernética encontra um proeminente campo de aplicação no ambiente militar. Não obstante, a aplicação de sistemas informacionais militares se amplifica muito após a década de 1950, produzindo uma profunda aceleração dos processos logísticos e sistemas de armas militares.

Essa aceleração tem efeitos políticos complexos no campo de batalha e além dele. Inicialmente, a aceleração informacional pela cibernética resulta no distanciamento físico dos combatentes do campo de batalha, graças à crescente automação e ao controle remoto de sistemas de armas. Esse distanciamento, mediado por sistemas informacionais e imagéticos, cria uma "guerra virtuosa" na qual a destruição e a morte causadas por novas armas autônomas ou controladas remotamente são frequentemente invisíveis socialmente, levando a práticas de violência mais extremas (Der Derian 2009). Além disso, a aceleração informacional da cibernética aprimora os sistemas de comando e controle militar, passando de uma estrutura hierárquica centralizada para um modelo complexo, flexível e descentralizado que integra sistemas computacionais e informacionais para melhorar a comunicação militar, prontidão e mobilização, bem como a eficácia no direcionamento das forças (Peron 2019).

Diante dessa diversificação dos mecanismos de comando e controle graças à sofisticação dos mecanismos cibernéticos, Bousquet (2022) sustenta que estaríamos diante de um novo regime de guerra científica, que ele denomina "Caopléxica". Este regime é orientado para o governo de ambientes altamente complexos e, em um mundo globalizado cravejado de ameaças difusas, sendo caracterizado pela descentralização dos conflitos, sua organização sob a forma de enxames e uma crescente autonomia dos sistemas de armas, vigilância, extração e triagem de informações — apoia-

dos em mecanismos estatísticos e matemática não linear para a amplificação da predição dos movimentos inimigos. Esse regime de guerra, pautado em uma organização dependente de aplicações de sistemas autônomos de armas, e de redes sofisticadas de vigilância, extração e otimização de informação é o que inspira os ideais de guerra centrada em rede e os modelos de contra insurgência da guerra global ao terror.[2]

Esse regime e base tecnológica, no entanto, não permanecem restritos à gestão da guerra e dos instrumentos militares no campo de batalha. O discurso e imaginário militarista (principalmente a estadunidense), dos anos 1970 e 1980 dos EUA, já colocavam a ideia de ameaças difusas e assimétricas como objetos de interesse militar, e nos anos posteriores aos atentados de 11 de setembro, esse discurso que incorpora o terrorismo como objeto de ação marcial amplifica a gestão militar sobre espaços, ambientes e pessoas que não aqueles habituais — como cidades, agrupamentos, organizações, empresas, indivíduos.

Nesse espectro, Harcourt (2021) irá entender que as técnicas e tecnologias deste regime é que viabilizaram e dão substância para a construção das estratégias de contrainsurgência estadunidense, nas quais se mesclam técnicas policialescas e marciais para o gerenciamento do cotidiano. O que estaria em desenvolvimento, nesse sentido, com a aplicação de sistemas de vigilância e monitoramento, reconhecimento facial, bases de dados e sistemas de extração e produção de informações e sistemas autônomos de armas dispostos globalmente seria um modelo de governo de populações.

"A guerra de contra insurgência tornou-se o novo paradigma de governo nos Estados Unidos, tanto no exterior quanto no âmbito interno" (Harcourt 2021, 21). Em outras palavras, seria o modelo da guerra, persecutório, violento, e intrusivo, justificado como tática de contra insurgência, se fundando como mecanismo de controle social. Essa forma de governo social militarista se centra em três eixos fundamentais, que se assemelham ao regime "Caopléxico": a) a busca pela obtenção total de informações (sobre indivíduos, organizações, dentre outros); b) A busca pela eliminação de uma minoria ativa (radicalizada, buscando eliminar os desviantes); c) por fim, a conquista da lealdade da população em geral (convencendo-a da virtuosidade das práticas e tecnologias aplicadas às caçadas humanas da contrainsurgência).

No século XX, as tecnologias de guerra, influenciadas pela cibernética e pela tecnologia da informação, transformaram a natureza da guerra, resultando em um aparato de controle global intrusivo, arbitrário e permanente. Essas tecnologias, como monitoramento, sistemas autônomos e comunicação, não se limitam ao campo de batalha, afetando também a vida social, urbanização e policiamento. Isso foi resultado da interação entre agentes

públicos e privados, incluindo empresas, militares, policiais e pesquisadores, a partir da Revolução nos Assuntos Militares (RAM) nos EUA, nos anos 1980, gerando inovações tecnológicas desde então (Graham 2016).

Os articulistas da RAM por diversas vezes manifestavam a intencionalidade em amplificar os meios militares disponíveis — principalmente por questões de custos e eficiência — para a gestão e adequação do urbano enquanto espaços "governáveis" (Graham 2006). Nesse sentido, as tecnologias de cunho militar, desde então, podem ser pensadas enquanto imersas em uma intencionalidade política explícita de dualidade, e implícita por maior autoridade. A cosmotécnica da RAM reflete essa busca pela ampliação de formas de controle e regulação social no modelo de contrainsurgência. Essa autoridade se manifesta não apenas como maior capacidade de emprego de força e violência por agentes de segurança ou privados, mas também na crescente invisibilidade e das tecnologias que viabilizam essas estratégias, e na consequente perda de autonomia humana diante do ganho de processamento e automatismo desses sistemas empregados para o controle social. Esse processo tem se intensificado e fica mais claro quando analisarmos o papel e os riscos das aplicações marciais-policiais da IA.

IA, POTENCIAIS E RISCOS

As aplicações militaristas e securitárias de sistemas de Inteligencia Articifical (IA) tem crescido muito nos últimos anos. De acordo com um levantamento da Vantage Market Research (2022), o mercado de aplicações militares da IA tende a ser de 13,71 bilhões de dólares até 2028. Conforme exploraremos, são diversas as formas de aplicação da IA para fins militares ou securitários, e, de certa forma, é possível afirmar que elas sejam a consolidação desse regime tecnológico "Caoplexico", onde se busca amplificar a difusão de sistemas de armas autônomas, e sistemas tecnológicos intrusivos, alinhados à coleta e processamento de dados para a identificação e eliminação de "ameaças", ao mesmo tempo em que se constroem dispositivos de vigilância e monitoramento para o gerenciamento e controle social. A IA estaria ancorada em uma cosmotécnica particular, onde se legitima o desenvolvimento de sistemas alinhados a projetos autoritários.

Desde meados da década de 1980, com a popularização de sistemas computacionais pessoais, com o avanço da Internet e o barateamento de sistemas informacionais capazes de coletar e processar uma grande quantidade de dados em um curto período (Big Data, IA, Deep Learning), muitos autores têm afirmado que entramos em um era do capitalismo informacional (Castells 1999). Nesse cenário, Big Data, a Inteligência Artificial, e os sistemas de Internet móvel tornaram os dados o elemento central na

acumulação de capital. Máquinas virtuais como o Big Data e a Inteligência Artificial se tornaram cruciais para a acumulação de capital, permitindo a coleta e processamento em grande escala de dados, bem como a geração de correlações para fazer previsões e inferências sobre padrões e interesses, seja em consumo, circulação e muito mais.

O termo "máquinas virtuais" para se referir à IA denota uma característica central desses aparatos, o fato de serem "sistemas de processamento de informações", que buscam a solução de problemas através de códigos de programação, e instruções traduzidas para o código da máquina para sua execução. Em geral, a IA envolve técnicas de programação e algoritmos que prepararam os computadores para realizar atividades que a mente é capaz de fazer, como raciocínio, habilidades psicológicas — como percepção, associação, previsão, planejamento, controle motor — para atingir determinados objetivos (Boden 2020, 13). O Ato Europeu sobre a Inteligência Artificial a define como "um software desenvolvido a partir de uma ou mais técnicas e abordagens [...] e que pode, dado um conjunto de objetivos humanos definidos, gerar resultados como conteúdos, predições, recomendações ou decisões, influenciando os ambientes nos quais elas interagem" (European Comission 2021).

Dessa forma, a IA é mais bem definida pelo conjunto de técnicas computacionais empregadas que permitem a máquina "aprender" e automatizar processos de correlação e associação, e fazer inferências a partir de então. Essas técnicas se desenvolveram a partir das inovações computacionais do século XX, ganhando expressão com a revolução informacional da cibernética, com os trabalhos sobre a "causação circular" ou *feedback*. No entanto, ela se "materializa" e se consolida principalmente a partir da viabilização e barateamento das técnicas de Big Data, que permitem a assimilação massiva de dados, e a construção de processos de aprendizado profundo e autônomo das máquinas virtuais.

Essas diferentes técnicas fazem com que a IA possa ser subdividida em 5 tipos gerais, a Gofai (sigla de *Good Old Fahshion AI*); redes neurais artificiais; programação evolutiva; autômatos celulares e os sistemas dinâmicos. Esses diferentes arranjos da IA, somados a computadores extremamente potentes, permitem com que as máquinas virtuais consigam solucionar problemas de forma extremamente eficiente (Boden 2020, 19). Isso se traduz na capacidade heurística da máquina: ou seja, dirigir atenção para um espaço de busca específico; sugerir espaços menores de busca e ordená-la eficientemente; ou reorientar a busca representando o problema de modo diferente a partir de associações (Boden 2020, 39). Outros exemplos de solução de problemas perpassam uma capacidade da IA em produzir planejamentos eficiente; programas baseados em regras; a visão computacional;

e, por fim, o aprendizado da máquina (em suas dimensões supervisionadas, com a ação humana "treinando" o processo estatístico de associações) (Boden 2020, 68–9).

Apesar de toda a enorme potencialidade da IA, esse fetichismo relativo à ideia de inteligência e automação das máquinas — que as alocaria em uma situação de objetos dotados de uma inteligência própria — tem sido colocado em xeque recentemente. Crawford (2021) explora a IA, não apenas enquanto um sistema contido em uma máquina e limitado pelas contingências de seu desenvolvimento programático, mas também como um sistema planetário, reflexo das disputas, tensões e vicissitudes sociais e relações econômicas diversas: "[...] *I argue that AI is neither artificial nor intelligent. Rather, artificial intelligence is both embodied and material, made from natural resources, fuel, human labor, infrastructures, logistics, histories and classifications*" (Crawford 2021, 8).

Assim, a IA estaria emaranhada em sistemas humanos políticos e econômicos existentes, potencialmente alinhadas à cosmotécnicas e imanências políticas autoritárias. Nesse sentido, os problemas que ela busca resolver, os modos de ver que ela viabiliza estariam designados a servir interesses de grupos dominantes, sendo assim, um registro de poder.

Não obstante, nessa condição, as aplicações marciais e policialescas da IA intensificam a crescente hibridização militarista, consolidando o modelo de guerra como forma de governo social. A partir do fetichismo que recobre as noções de automação e inteligência que, mesmo diante da violência e arbitrariedade promovida pelas tecnologias de contrainsurgência, tem se espraiado uma aceitação passiva do assujeitamento cibernético, conforme preconizado por Virilio.

Nesse contexto, Boden e Crawford apontam o modo como o Pentágono, e as empresas privadas de segurança, têm sido os setores que mais investem no desenvolvimento da IA e em aplicações possíveis no campo securitário. Já durante a RAM, várias iniciativas que envolviam aplicações de inteligência artificial passaram a ser testadas, como sistemas autônomos, e sistemas de radares e de mísseis inteligentes. Nesse sentido, Svenmarck et al. (2018) e Eliaçik (2022) buscaram relacionar diversas aplicações militares da IA, e explorando algumas das suas potencialidades e limites. Em geral, descrevem aplicações como sistemas inteligentes de vigilância e monitoramento marítimo; sistemas de minas marítimas inteligentes; sistemas de cyber-segurança (capazes de classificar, identificar padrões anormais de tráfego, atacando-os de forma seletiva); gerenciamento logístico; sistemas de reconhecimento de alvos aplicados a sistemas de armas, veículos autônomos e radares; sistemas de treinamento e simulação de combate; sistemas de gerenciamento de

saúde mental; e evidentemente, sistemas de detecção e monitoramento de consciência situacional.

Alguns dos problemas aviltados para essas aplicações no campo militar envolvem, principalmente, a falta de participação humana nos processos de aprendizado, criatividade e arbítrio diante de situações adversas, falta de explicabilidade e transparência (Asaro 2019). No entanto, os riscos relativos a essa progressiva autonomização de sistemas graças a IA vão muito além desses erros, e envolvem sérios dilemas securitários, que extrapolam os limites das aplicações militares.

Yu e Pashentsev (2019) articulam uma discussão a respeito dos chamados usos maliciosos da inteligência artificial para descrever os riscos à segurança psicológica. Tais usos maliciosos da IA envolvem uma miríade de aplicações, que podem produzir riscos sociais diversos e abalar os processos de desenvolvimento político e econômico de um país, como o crescimento de infraestruturas dependentes de IA, e que ficam abertas a ações de *hackers* ou de "terroristas"; vírus baseados em IA, como o Deeplocker da IBM, que poderia ser destinado a afetar essas infraestruturas; a reorientação de sistemas comerciais de IA para fins maliciosos; ataques remotos com sistemas de armas autônomas; a criação de *deepfakes*, pessoas falsas e direcionamento de agendas para a produção de desinformação; sistemas preditivos e os riscos de prisões arbitrárias. Não obstante, a definição de usos maliciosos da IA pode ser expandida para sistemas de armas, sistemas de vigilância baseadas em IA — como reconhecimento facial e policiamento preditivo — que podem incorporar vieses ou viabilizar práticas violentas e intrusivas.

Justamente nesse contexto de diversas ameaças o *AI Incident Database* descreve e analisa uma série incidentes relacionados às aplicações militares, policiais, e de outras ordens da IA no mundo todo. Ainda que apenas 26,9% das funções da IA estejam relacionadas a uma ação direta (sendo 37,8% relacionadas à cognição e 31,6% à percepção), a gravidade de incidentes varia da seguinte forma: 46% deles estão relacionados com negligências e inconvenientes menores, enquanto 17% estão entre moderados e graves, que envolvem desde injurias médias e graves sobre humanos. Essa substantiva gravidade tem sido protagonizada por diversos setores, dentre os quais informação e comunicação (29,4%); artes, entretenimento e recreação (15,3%); transporte e armazenamento (11,8%); e administração pública e defesa (10,6%), havendo outros setores menos relevantes para a nossa análise. O setor de defesa e policiamento tem uma relevante participação na produção de incidentes, e envolvem práticas policiais racializadas, prisões arbitrárias, identificações errôneas, erros do sistema judiciário, falsos alarmes de ataques nucleares, erros de sistemas autônomos de armas etc.

Da guerra ao controle social: os usos da IA

No final da década de 1980, com o imponente programa militar promovido pelo governo Reagan (a RAM), tornou-se cada vez mais comum um discurso de guerra cirúrgica e rápida tanto nos quartéis quanto nos corredores do Pentágono. Esse discurso, constituído pelas novas doutrinas de "Network Centric Warfare" e em meados dos anos 1990, "*Shock and Awe*", afirmava que seria possível às forças armadas dos Estados Unidos conduzir conflitos de baixa intensidade, com apenas alguns "efeitos colaterais". Consequentemente, graças às novas tecnologias de informação e comunicação, as guerras se tornariam supostamente menos destrutivas e mais precisas. Esse reordenamento enquadra os drones, como o Predator MQ-1, como importantes veículos de vigilância e coleta de informações para otimizar as operações militares.

As execuções extrajudiciais com drones são organizadas de duas maneiras. Primeiro, por meio de assassinatos seletivos, em que as operações são voltadas para a eliminação de alvos muito específicos com base no trabalho de oficiais de inteligência em campo, bem como dados coletados a partir da triagem de imagens realizadas por drones. Outro método seria o assassinato por sinais (indícios gerais), neste caso, como diz Chamayou (2013, 72–3), baseia-se na visualização de "alvos" e cruzamento de dados diversos (geolocalização, telefônicos etc.), identificando padrões suspeitos.

Desde 2012, o Pentágono vem desenvolvendo o sistema de IA chamado Skynet para processar dados de drones, analisando padrões e comunicações de alvos, incluindo informações de redes sociais. Os drones fazem parte de uma cadeia de comunicação chamada "Kill Chain", e a IA utiliza técnicas de mineração de dados e perfilização para uma visão mais precisa dos alvos com base em dados e metadados (Currier et al. 2015). Ademais, desde 2017, o Pentágono investe em parcerias público-privadas para realizar projetos como o "Maven", que tenta incorporar IA e aprendizado profundo para detecção e reconhecimento automático de suspeitos em vídeos de drones militares. No entanto, como detalha Crawford (2021, 189), o programa visava a estimular parcerias entre o Pentágono e as Big Tech, detentoras de bases de dados de reconhecimento facial, como Google e Microsoft, para a partir de então tornar os algoritmos de reconhecimento biométrico dos drones mais sofisticados, e assim detectar combatentes inimigos de forma mais rápida. Entidades de defesa dos direitos humanos e a comunidade acadêmica passaram a questionar a capacidade desse sistema em assegurar o cumprimento das normas essenciais de conduta em conflitos, bem como os princípios do direito humanitário internacional (Clark and Mcleary 2018).

Nesse contexto, tanto os EUA como Israel têm ampliado o emprego de IA para aprimorar a autonomia de seus sistemas de armas para a identificação e eliminação de alvos. No entanto, por diversas vezes, essa maior automação pode se chocar com limites humanitários em conflitos, como apontam Asaro (2019), Suchman (2020) e Chamayou (2013). Para estes autores, atribuir autonomia a sistemas de armas para decisões letais não é apenas um dilema ético, como também uma demonstração de autoritarismo na trajetória tecnológica desses instrumentos, que incide no desrespeito aos princípios de proporcionalidade e distinção no conflito. Isso porque os processos de automação eliminam o arbítrio dos operadores em decisões complexas no campo de batalha; lega a um universo de programadores e empresas não militares a autoridade para atribuir aos algoritmos as decisões sobre condutas suspeitas, nocivas, inimigas — que podem induzir a eliminação de alvos; acima de tudo, podem induzir operadores ao erro em ações letais, posto que processamentos falhos de dados (que podem ser enviesados) podem acabar por construir inimigos em sistemas de alvos.

Como um exemplo avassalador desse emprego nocivo de sistemas de IA, podemos destacar o sistema Lavender, desenvolvido pela Elbit Systems e empregado pelas Forças de Defesa de Israel em Gaza. O sistema processa dados coletados por drones — como o SkyStriker — e outros múltiplos sensores, conseguindo assim detectar padrões e classificar objetos (veículos, pessoas, atividades e condutas de pessoas e outras entidades), destacando anomalias e desvios nesse processo. Quando isso ocorre, o sistema dispara um alerta para munir operadores de drones e demais militares de informações, ou, em certos casos, ele mesmo pode acionar sistemas de armas sem o consentimento humano, ao identificar alvos ou condutas suspeitas.[3] Considerando que o sistema se caracteriza por ser um modelo probabilístico, ele trabalha a partir de estimativas, com base em dados estatísticos — e não apenas informações concretas sobre supostos combatentes — e, de acordo com uma investigação realizada pelo The Guardian (McKernan and Davies 2024), em torno de 37 mil palestinos teriam sido identificados enquanto potenciais alvos, dos quais em torno de 15 mil podem ter sido eliminados a partir desse sistema probabilístico (Pascual 2024).

Desse modo, é importante destacar que processos baseados em IA para munir sistemas preditivos mobilizam dados do passado como evidências concretas para o estabelecimento de previsões sobre o futuro. Nesse contexto, há um enorme risco, pois, a partir de uma estatística preditiva, devidamente ancorada e apoiada em discursos de guerra justa e eminência de ataques terroristas, autoriza ataques preventivos contra alvos em outros países. Mais do que isso, ao tornar visíveis padrões de comportamento, conexões e associações, o sistema "faz surgir" inimigos e insurgentes, fundamentando

"[...] a suspeita que o analista de segurança já tem, em vez de prever novos suspeitos ou comportamentos suspeitos" (Aradau and Blanke 2015).

Paralelamente, desde a década de 1990, Garland (2008) identificou o surgimento de uma "nova cultura de controle" nos Estados Unidos e no Reino Unido. Nessa cultura, as práticas de vigilância policial não se limitam mais aos suspeitos, mas se estendem a todos os cidadãos, visando a identificar potenciais perturbações futuras, como comportamentos suspeitos em toda a cidade, com foco em áreas problemáticas. De maneira similar, como analisa Feldstein (2021), nos últimos 20 anos, uma série de países sob regimes autoritários — ou que tem passado por governos antidemocráticos — tem recorrido a expedientes relacionados à repressão digital e ao emprego de aparatos de contrainsurgência para a administração da segurança pública. Estes têm intensificado esse modelo policial centrado no vigilantismo, com base em um conjunto de sistemas (híbridos militares e policiais) de vigilância baseados em IA — como de policiamento preditivo, reconhecimento facial, de classificação de riscos, dentre outros.

Este ambiente, cuja produção de informações é extremamente ampla, exige a adoção de doutrinas, dispositivos e estruturas que permitam maior capacidade de "consciência situacional" da polícia. Isso se intensificou após os atentados de 11 de setembro, com maior circulação de tecnologias, discursos e conceitos operacionais advindos da RAM no meio policial estadunidense (Harcourt 2021), fruto de uma mediação entre os setores militar e policial promovida por órgãos governamentais, empresas privadas, empresas de gestão de riscos e consultorias que, em uma rede de "especialistas", atuam na produção de consensos e discursos que conectam a segurança interna e internacional, fundindo iniciativas para combater o crimes e o terrorismo em um mesmo *continuum* de (in)segurança (Peron 2021).

Assim, as iniciativas de contrainsurgência passam a se amparar na aplicação de uma série de tecnologias de vigilância baseadas em IA, como o sistema Predpol, da polícia de Los Angeles. Essa iniciativa traduz demandas complexas de hipervigilância, identificação de inimigos e "comportamentos suspeitos", bem como a probabilidade de ocorrência de crimes, por meio de algoritmos preditivos. O Predpol (sigla para Policiamento Preditivo) é um software que opera com base em algoritmos preditivos e é projetado para analisar estatísticas criminais passadas, integrando vários bancos de dados criminais e legais para gerar probabilidades de ocorrências de crimes futuros em várias regiões da cidade. Nesse caso, as atividades policiais são pautadas por essa dinâmica de atualização do risco de crimes futuros e na atualização de condutas suspeitas futuras.

No entanto, essas "soluções" têm sido alvo de muitas dúvidas e questionamentos por parte de pesquisadores, autoridades e associações, pois

tendem a reforçar e legitimar práticas policiais discriminatórias, principalmente em comunidades mais vulneráveis. Um estudo da Universidade de Utah (Ensing et al. 2018), por exemplo, mostra que Predpol sofre do "*feedback loop*". Ou seja, esses sistemas baseados em dados e estatísticas passadas tendem a punir comunidades vulneráveis, principalmente quando essa tecnologia se baseia em bancos de dados criminais que há anos são abastecidos com dados dessa mesma comunidade, gerando um "*loop*" perpétuo na probabilidade de ocorrência de crimes nas mesmas regiões. O Predpol torna visíveis e atualiza os riscos aos quais as cidades estariam expostas, mobilizando estatísticas, dados, informações, imagens, por meio de algoritmos preditivos ou alertas analíticos. Esses sistemas normalizam mecanismos de sujeição, exclusão e segregação de parcelas significativas da população. Isso implica que os vieses que caracterizam o "*feedback loop*" não podem ser entendidos como erros de forma alguma, mas sim como um manifesto de intencionalidade política contido na própria IA.

Por sua vez, durante o governo Netanyahu, diversas agencias de proteção dos direitos humanos têm denunciado um uso sistemático de drones de vigilância, de sistemas de reconhecimento facial e de *spywares* como forma de monitoramento da população na Cisjordânia (Fatafta 2023; Amnesty 2023). Conjuntamente com os conhecidos *checkpoints* e políticas de assujeitamento de colonos, esses aparatos estruturam uma ação de gestão urbana contrainsurgente violenta e discriminatória. De acordo com o relatório da anistia Internacional, "*apartheid* automatizado" (Amnesty 2023), essa prática tem se intensificado a partir do emprego massivo em Hebron — principalmente em bairros palestinos — de torres de vigilância, detectores de sons, de sistemas de vigilância estruturados em casas de colonos, mas fundamentalmente de sistemas de reconhecimento facial automatizado, a partir do projeto denominado "Wolf Pack". Este projeto, desenvolvido pelo exército israelense — com o acesso do Shin Bet —, consiste em uma enorme base de dados, exclusivamente de palestinos, com perfis, redes de relacionamento e comunicação, gerando um método intrusivo de coleta de dados. Esse sistema está associado, ainda, aos sistemas Blue Wolf e Red Wolf. O primeiro é um sistema de reconhecimento facial aplicado a dispositivos móveis ou a sistemas de câmeras, permitindo a identificação e coleta instantânea dos dados biométricos de um individuo na base de dados Wolf Pack. Por sua vez, o segundo, é um sistema de vigilância baseado em IA aplicado principalmente em regiões de fronteiras, nos assentamentos e *checkpoints*, que integra sistemas de imagem e de sensoriamento para a identificação de padrões e predição de ações (Amnesty 2023). Isso não apenas intensifica um processo de *apartheid* em grandes cidades, como produz efeitos psicológicos severos nos cidadãos, erodindo a vida social, restrin-

gindo o espaço de circulação de palestinos na cidade e ampliando os meios para a repressão e perseguição de ativistas.

CONCLUSÕES

A busca por aperfeiçoar a logística e a precisão na guerra levou à introdução massiva de sistemas tecnológicos para aumentar a previsibilidade e estabilidade nas estratégias de segurança. Esses sistemas transformaram forças de segurança em centros de processamento de informações, descentralizando as operações. A "Guerra Global ao Terror" estabeleceu práticas intrusivas de espionagem e predição que misturaram policiamento e militarismo, resultando em um complexo mecanismo de governo social. O uso de sistemas de vigilância baseados em IA tornou-se essencial para a contra insurgência.

A IA aplicada para práticas de vigilância e monitoramento, portanto, se estrutura em torno de imanências políticas e cosmotécnicas autoritárias. Por um lado, o desenvolvimento da IA segue um modelo extremamente predatório, fundado nas práticas extrativistas e produtivas que reforçam a tensão entre capital e trabalho, a divisão internacional desigual do trabalho. Por outro, como buscamos demonstrar aqui, o emprego da IA para fins securitários se dá em um contexto de ampliação (espacial e temporal) das práticas policiais e militares em um governo social abrangente e intrusivo, orientado não apenas para identificar a autuar ameaças, como também para construí-las (predizê-las).

As práticas preditivas que têm sido viabilizadas pelo emprego securitário da IA se manifestam enquanto autoritárias, uma vez que viabilizam a antecipação e pressuposição de culpa dos alvos, permitindo ações militares e policiais sem o devido respeito a direitos fundamentais. Ao viabilizar uma política de detenção antecipada ou das "ameaças", as tecnologias preditivas reforçam um estado de permanente suspeita e desconfiança, no qual a hipótese de punição sustentada por uma dinâmica de coleta de dados induz a mudança nos comportamentos e práticas sociais. Mais ainda, o contorno autoritário se manifesta na instauração de um ambiente de reduzidíssima transparência sobre o funcionamento dessas tecnologias, de seus limites, e com o envolvimento entre atores sem as devidas responsabilidades legais sobre as práticas de segurança.

A consequência tem sido a crescente infiltração de modelos de elevada intrusividade e de violência desregulada estruturando a arquitetura, as práticas sociais, as leis e o cotidiano da vida social. O estudo a respeito das interações sociais das tecnologias securitárias, mais do que explicitar os aprimoramentos estratégicos da guerra pelo emprego de novas tecnologias,

torna-se fundamental para compreender as imanências políticas de seu desenvolvimento e os efeitos sociais que elas viabilizam, para somente assim avaliá-las e desenvolver mecanismos para a mitigação dos seus efeitos.

REFERÊNCIAS

Amnesty International. 2023. *Automated Apartheid: How Israel's Surveillance Regime Is Enabling Apartheid*. London: Amnesty International, www.amnesty.org/en/documents/mde15/6701/2023/en.

Aradau, Claudia, and Tobias Blanke. 2015. "The (Big) Data-security assemblage: Knowledge and Critique". *Big Data & Society*.

Asaro, Peter. 2019 "Algorithms of Violence: Critical Social Perspectives on Autonomous Weapons". *Social Research* 86, no. 2: 537–55.

Boden, Margareth. 2020. *Inteligência Artificial: Uma Brevíssima introdução*. São Paulo: Editora Unesp.

Bourdieu, Pierre. 2004. *Os Usos Sociais da Ciência: Por uma sociologia clínica do campo científico*. São Paulo: Editora Unesp.

Bousquet, Antoine. 2022. *The Scientific Way of Warfare: Order and chaos on the Battlefields of Modernity*. Oxford: Oxford University Press.

Castells, Manuel. 1999. *A sociedade em rede*. 3. ed. São Paulo: Paz e Terra.

Chamayou, Gregóire. 2013. *Théorie du Drone*. Paris: La Fabrique.

Clark, Colin, and Patrick Mcleary. 2018. "Legal Scholars, Software Engineers Revolt Against War Robots". *Breaking Defense* (Abr.). breakingdefense.com/2018/04/a-treaty-to-ban-autonomous-intelligence-weapons.

Crawford, Kate. 2021 *Atlas of AI: Power, Politics and the Planetary Costs of Artificial Intelligence*. London: Yale Univarsity Press.

Currier, Cora, Glenn Greenwald, and Andrew Fishman. 2015. "U.S. Government Designated Prominent Al Jazeera Journalist as 'Member of Al Qaeda'". *The Intercept* (Maio) theintercept.com/2015/05/08/u-s-government-designated-prominent-al-jazeera-journalist-al-qaeda-member-put-watch-list.

Der Derian, James. 2009. *Virtuous War: Mapping the Military-Industrial Media Entertainment Network*. Nova Iorque: Routledge.

Der Derian, James. 2019. *Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network*. 3. ed. Nova York: Routledge.

Eliaçik, Emre. 2022. "Guns and Codes: The Era of AI-wars begins". *Dataconomy* (Ago.). dataconomy.com/2022/08/how-is-artificial-intelligence-used-in-the-military/#Disadvantages_of_artificial_intelligence_in_the_military.

Ensing, David, Sorelle Friedler,, Scott Neville,, Christian Scheidegger, and Suresh Venkatasubramanian. 2018. "Runaway Feedback Loops in Predictive Policing". *Proceedings of Machine Learning Research* 81.

European Commission. 2021. *The European approach to Artificial Intelligence*. ec.europa.eu/commission/presscorner/detail/en/ip_21_1682.

Fatafta, Marwa. 2023. "Apartheid Tech: The use and expansion of biometric identification and surveillance technologies in the occupied West Bank". In *Resisting Borders and Technologies of Violence*, edited by M. Aizeki, M. Mahmoui, and C. Schupfer. Chicago: Haymarket Books.

Feldstein, Steven. 2021. *The Rise of Digital Repression: How Technology is reshaping power, politics, and resistance*. Oxford: Oxfornd University Press.

Garland, David. 2008. *A cultura do controle: crime e ordem social na sociedade contemporânea*. Rio de Janeiro: Editora Revan.

Graham, Stephen. 2006. "Surveillance, urbanization and the US "Revolution in Military Affairs". In *Theorizing Surveillance: The panopticon and beyond*, edited by D. Lyon: 247–69. Cullompton, Portland: Willan.

Graham, S Stephen. 2016. *Cidades sitiadas: o novo urbanismo militar* São Paulo: Boitempo.

Gros, Fréderic. 2008. *Estados de Violência: Ensaio sobre o fim da guerra*. Aparecida, SP: Editora Ideias & Letras.

Hansen, Lene, and Helen Nissembaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School". *International Studies Quarterly* 53.

Harcourt, Bernard E. 2020. *A contrarrevolução: como o governo entrou em guerra contra os próprios cidadãos*. São Paulo: GLAC Edições.

Hughes, Thomas. 2012. "The Evolution of Large Technological Systems". In *The Social Construction of Technological Systems: New Directions in the History and Sociology of Technology*, edited by Wiebe Bijker, Thomas Hughes, and Trevor Pinch. Cambridge: MIT Press.

Huk, Yuk. 2020. *Tecnodiversidade*. São Paulo: Editora Ubu.

Keagan, John. 2006. *Uma História da Guerra*. São Paulo: Companhia das Letras.

Khun, Thomas. 2017. *A Estrutura das revoluções Científicas*. São Paulo: Perspectiva.

Latour, Bruno, and Steve Woogar. 1988. *A vida de laboratório: a produção dos fatos científicos*. Rio de Janeiro: Relume Dumará.

Mackenzie, Donald, and Judy Wajcman. 1999. "Introductory essay: the social shaping of technology". In *The Social Shaping of Technology*, edited by D, Mackenzie and J. Wajcman. Filadélfia: Open University Press.

Marx, Karl. 2011. *O capital: crítica da economia política*. Rio de Janeiro: Civilização Brasileira.

McKernan, Benthan, and Harry Davies. 2024. "'The machine did it coldly': Israel used AI to identify 37,000 Hamas targets". *The Guardian* (Abr.). www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas-airstrikes.

Morgenthau, Hans. 1964. *Politics among Nations: The struggle for power and peace*. Nova Iorque: Knopf.

Pascual, Manuel. 2024. "Lavender, Israel's artificial intelligence system that decides who to bomb in Gaza". *El País* (Abr.). english.elpais.com/technology/2024-04-17/lavender-israels-artificial-intelligence-system-that-decides-who-to-bomb-in-gaza.html.

Pinch, Trevor, and Wiebe Bjiker. 2012. "The Social Construction of Facts and Artifacts: Or how the sociology of science and the sociology of technology might bennefit each other". In *The Social Construction of Technological Systems: New Directions in the History and Sociology of Technology*, edited by Wiebe Bijker, Thomas Hughes, and Trevor Pinch. Cambridge: MIT Press.

Rosenberg, Nathan. 1982. *Inside the Black Box — Technology and economics*. Cambridge: Cambridge University Press.

Srnicek, Nick. 2017. *Platform Capitalism*. Cambridge: Polity Press.

Stokes, Donald. 2005. *O Quadrante de Pasteur — a ciência básica e a inovação tecnológica. Clássicos da Inovação*. Campinas: Editora da Unicamp.

Suchman, Lucy. 2020. "Algorithmic Warfare and the Reinvention of Accuracy". *Critical Studies on Security* 8, no. 2: 175–87.

Svenmark, Peter, Linda Luotsinen,, Magnus Nillson, and Johan Schubert. 2018. "Possibilities and challenges for Artificial Intelligence in Military Application". *S&T Organization – OTAN.*

Van Creveld, Martin. 1991. *Technology and War: From 2000 B.B. to the Present.* Nova Iorque: The Free Press.

Vantage Market Research. 2022. "$13+ Billion Artificial Intelligence (AI) in Military Market is Expected to Grow at a CAGR of over 12.9% During 2022-2028". *Globe Newswire* (Abr.).

Velho, Lea. 2011. "Conceitos de Ciência e a Política Científica, Tecnológica e de Inovação". *Sociologias* 13, no. 26: 128–53 (Jan./Abr.). Porto Alegre.

Virilio, Paul, and Sylvere Lotringer. 1984. *Guerra pura: a militarização do cotidiano.* São Paulo: Editora Brasiliense.

Virilio, Paul. 2002. *A máquina de visão.* Rio de Janeiro: José Olympio.

Waltz, Kenneth. 2001. *Man, the state, and war: a theoretical analysis.* Nova Iorque: Columbia University Press.

Wierner, Norbert. 1988. *The Human Use of Human Beings: Cybernetics and Society.* Boston: De Capo Press.

Winner, Langdon. 1986. "Do Artifacts have Politics?" In *The Whale and the Reactor: A search for limits in an Age of High Technology*, edited by L. Winner. Chicago: The University of Chicago Press.

Yu, Doris, and Yuri Pashentsev. 2019. "Artificial Intelligence and New Threats to International Psychological Security". *Russia in Global Affairs* 17, no. 1: 147–70.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The fight for a human future at the new frontier of power.* London: Profile Books.

DA GUERRA À VIOLÊNCIA PERMANENTE: A IMANÊNCIA AUTORITÁRIA DAS TECNOLOGIAS SECURITÁRIAS BASEADAS EM IA

RESUMO

O emprego de tecnologias baseadas em Inteligência Artificial (IA) para subsidiar estratégias marciais e policialescas tem crescido muito nos últimos anos. Sistemas baseados em IA são responsáveis por remodelar as estratégias em conflito, mas, acima de tudo, eles também têm embasado modelos de controle social em um contexto de contrainsurgência — onde a gestão de ambientes urbanos, de interações sociais como forma de eliminar grupos radicais é um objetivo central. Em ambas as aplicações, no entanto, verifica-se um enorme potencial abusivo e intrusivo, capazes de colocar em risco a segurança e os direitos de pessoas e grupos. Nesse sentido, o objetivo deste artigo é explorar como as tecnologias baseadas em IA se baseiam em imanências políticas autoritárias, associadas a uma fase "caopléxica", conforme apontado por Bousquet (2022), e, dessa forma, tendem a ampliar formas repressivas e modelos abusivos de promoção da violência em conflitos. Para tanto, nos apoiamos nos Estudos Sociais da Ciência e da Tecnologia e nos estudos de filosofia e história da guerra, além de mobilizar dados e informações relativas a sistemas baseados em IA com potencial abusivo.

Palavras-Chave: Inteligência Artificial; Cibernética; Guerra; Controle Social

ABSTRACT

The use of technologies based on Artificial Intelligence (AI) to support martial and policing strategies has grown significantly in recent years. AI-based systems are responsible for reshaping conflict strategies, but above all, they have also underpinned models of social control in a counterinsurgency context—where the management of urban environments and social interactions as a means to eliminate radical groups is a central objective. In both applications, however, there is an enormous potential for abuse and intrusion, capable of jeopardizing the safety and rights of individuals and groups. In this regard, the aim of this article is to explore how AI-based technologies are grounded in authoritarian political immanences, associated with a "caoplectic" phase as pointed out by Bousquet (2022), and thus tend to expand repressive forms and abusive models of promoting violence in conflicts. To this end, we draw on Social Studies of Science and Technology, and studies in the philosophy and history of war, in addition to mobilizing data and information related to AI-based systems with abusive potential.

Keywords: Artificial Intelligence; Cybernetics; Warfare; Social Control

Recebido em 28/06/2024. Aceito para publicação em 16/08/2024.

NOTAS

1. Sobre isso, Virilio entende que tecnologias informacionais têm como seu principal "acidente", o perceptivo, dado que cada vez mais são empregadas de modo a corrigir os veises e limites de análise dos humanos, como sistemas de radares, sistemas de leituras de imagem, de câmeras inteligentes etc. O ser humano se rende diante da aceleração informacional dos sistemas computacionais, os quais produzem um descompasso entre a percepção humana e a da máquina.
2. Para Virilio (1984), já desde a gênese do Estado se percebia uma militarização do cotidiano, em que as tecnologias e formas de organização social são inspiradas pelo militarismo. "A classe militar é isto, esta espécie de inteligência desenfreada cuja ausência de limites provém da tecnologia, da ciência. A máquina de guerra não é só explosiva, também é comunicações, vetorização" (Virilio and Lotringer 1984, 27–8). A guerra é, para ele, o modelo social dominado pela tecnologia e inspirado pela classe militar, que desregula o espaço urbano e domina nossa consciência, um modelo flexível no qual se articulam técnicas de comando, controle e vigilância.
3. Ver mais em elbitsystems.com/product/skystriker/#:~:text=URL%3A%20https%3A%2F%2Felbitsystems,100.