RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.
Ano II, v.2 2022. | submissão: 11/11/2022 | aceito: 13/11/2022 | publicação: 15/11/2022

TECNOLOGIAS MILITARES NA SEGURANÇA PRIVADA: INOVAÇÕES E APLICAÇÕES

MILITARY TECHNOLOGIES IN PRIVATE SECURITY: INNOVATIONS AND APPLICATIONS

Autor: Rodrigo Hipólito Menezes de Araújo.

Formado em Direito, pela ULBRA - Universidade Luterana Brasileira

Pós-graduando em Direito Público, pela Universidade do Amazonas - UEA

Resumo

O presente artigo científico se propõe a investigar o fenômeno da transposição e adaptação de tecnologias e metodologias de origem militar para o setor de segurança privada no Brasil e no cenário global, analisando as implicações jurídicas e operacionais desta crescente militarização. O estudo detalha a incorporação de Veículos Aéreos Não Tripulados (VANTs), a customização de *softwares* de monitoramento com capacidade de inteligência e a aplicação de técnicas de *intelligence* militar ao contexto de gestão de riscos corporativos. O objetivo central é demonstrar como tais inovações elevam a eficiência na prevenção e resposta a ameaças, ao mesmo tempo em que suscitam dilemas éticos complexos relacionados à vigilância massiva e à preservação das garantias fundamentais da cidadania. Conclui-se pela urgência na atualização do marco regulatório nacional para compatibilizar a inovação tecnológica com os imperativos do Estado Democrático de Direito, especialmente no tocante à privacidade e aos limites do exercício do poder de polícia privado.

Palavras-chave: Segurança Privada; Militarização; Tecnologias de Duplo Uso; VANTs; Inteligência Corporativa; Direito Público.

Abstract

This scientific article aims to investigate the phenomenon of transposition and adaptation of military-grade technologies and methodologies into the private security sector in Brazil and globally, analyzing the legal and operational implications of this increasing militarization. The study details the incorporation of Unmanned Aerial Vehicles (UAVs), the customization of monitoring *software* with intelligence capabilities, and the application of military *intelligence*techniques to corporate risk management. The central objective is to demonstrate how such innovations increase efficiency in threat prevention and response, while simultaneously

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

raising complex ethical dilemmas related to mass surveillance and the preservation of fundamental guarantees of citizenship. The conclusion highlights the urgency of updating the national regulatory framework to reconcile technological innovation with the imperatives of the Democratic Rule of Law, particularly concerning privacy and the limits of the exercise of private policing power.

Keywords: Private Security; Militarization; Dual-Use Technologies; UAVs; Corporate Intelligence; Public Law.

1. Introdução: A Transposição Tecnológica e a Fronteira Difusa entre o Público e o Privado

A segurança, em sua concepção sociológica e jurídica, representa uma das mais elementares demandas sociais e um dos deveres primordiais do Estado, estabelecendo o monopólio legítimo da força como sustentáculo da ordem pública e da paz social; contudo, a incapacidade ou a insuficiência da ação estatal em atender plenamente a essa demanda, especialmente em contextos de alta complexidade urbana e de escalada da criminalidade organizada, engendrou um crescimento exponencial do setor privado de segurança, que historicamente se limitava à vigilância ostensiva e patrimonial de baixo custo e com reduzida incorporação tecnológica (SOARES, 2018). Este crescimento, verificado em escala global desde o final do século XX, veio acompanhado de uma transformação qualitativa na natureza dos serviços prestados, impulsionada por uma dinâmica de mercado que exige alta eficiência, precisão preditiva e, sobretudo, a minimização dos riscos inerentes à atividade, o que culminou na busca por *know-how* e equipamentos historicamente restritos ao domínio da defesa e das operações militares de alta *performance*, caracterizando, assim, um processo de militarização silenciosa e tecnologicamente mediada. Essa transposição tecnológica e metodológica das esferas de segurança e defesa para o âmbito corporativo e privado não pode ser analisada meramente como uma otimização operacional ou uma estratégia de *marketing* empresarial, mas sim como um fenômeno sociopolítico que desestabiliza a clássica distinção entre o aparato de coerção pública e as atividades de proteção patrimonial, exigindo uma reavaliação crítica dos limites do poder de vigilância e das implicações jurídicas dessa transferência de *expertise* e instrumental bélico adaptado.

O cerne da presente investigação reside na análise detalhada de como recursos de dupla utilização, originalmente desenvolvidos e aprimorados em teatros de operações militares e em ambientes de inteligência estratégica, são adaptados e incorporados pelas empresas de segurança privada para fazer frente a ameaças que também se sofisticaram, como o roubo de cargas de alto valor agregado, a invasão de *data centers* ou a proteção de grandes infraestruturas críticas, as quais demandam soluções que superam em muito a capacidade operacional da segurança humana convencional (TILLY, 1985). A incorporação de *drones* (VANTs) para patrulhamento perimetral e o uso de *softwares* de análise preditiva com base em algoritmos de reconhecimento facial ou de padrões

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

comportamentais, que por sua vez encontram suas raízes em sistemas militares de comando e controle, são exemplos paradigmáticos dessa simbiose tecnológica que redefine o panorama da segurança. A problemática central, portanto, não reside na licitude da tecnologia em si, mas na ausência de um arcabouço normativo que consiga acompanhar a velocidade da inovação, gerando um vácuo regulatório onde o poder de vigilância privada pode ser exercido sem o devido controle social e sem a salvaguarda eficaz dos direitos de privacidade, intimidade e imagem dos cidadãos, conforme preconiza a Constituição Federal de 1988 (BRASIL, 1988).

É imperativo, pois, que a academia e o Direito Público se debrucem sobre a natureza e as consequências dessa absorção tecnológica, compreendendo que a eficiência na redução de riscos para o setor privado não pode ser alcançada à custa da descaracterização do regime de proteção dos direitos fundamentais, sendo a presente análise conduzida com um rigor metodológico que busca equilibrar a descrição das inovações operacionais com a crítica jurídica e ética inerente à temática (SANTOS, 2017). A estrutura deste artigo foi concebida para examinar, em seus capítulos subsequentes, os instrumentos tecnológicos e metodológicos transferidos, as implicações jurídicas de sua aplicação e, finalmente, os dilemas éticos que essa ampliação da capacidade de vigilância e de coleta de dados impõe à sociedade civil e ao próprio conceito de segurança como um bem público, culminando em uma reflexão ampliada sobre a necessidade de regulamentação urgente e específica.

2. O Paradigma Tecnológico e a Convergência Militar-Privada na Gestão de Riscos

O conceito de **tecnologias de duplo uso** (dual-use technologies) funciona como o principal vetor teórico para entender a rápida absorção de *hardware* e *software* militares pelo segmento de segurança privada, sendo essas tecnologias caracterizadas pela sua aplicabilidade tanto em contextos bélicos ou de defesa nacional quanto em aplicações civis ou comerciais, facilitando a migração do conhecimento e dos equipamentos desenvolvidos com fundos públicos de pesquisa militar para o mercado aberto de segurança (PEREIRA, 2019). Este processo não é acidental, mas sim um reflexo da reestruturação do complexo industrial-militar após a Guerra Fria, período em que houve uma desmobilização de *expertise* e um excedente de tecnologias que, para encontrarem um novo mercado, foram simplificadas, barateadas e adaptadas para atender à crescente demanda por proteção em um ambiente corporativo globalizado, onde os riscos operacionais, logísticos e de imagem se tornaram prioridade para os grandes conglomerados empresariais e para os proprietários de infraestruturas críticas (HARTZ, 2015). Essa convergência é notória em áreas como a sensoriamento remoto, a robótica e a análise de grandes volumes de dados (*Big Data*), campos onde o investimento militar maciço resultou em ferramentas de monitoramento e vigilância com precisão incomparável.

A lógica que impulsiona essa absorção reside, fundamentalmente, na superioridade técnica e na confiabilidade dos equipamentos militares e de defesa, projetados para operar sob condições extremas e para realizar a detecção e o rastreamento de alvos com margem de erro mínima,

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

características que são traduzidas para a segurança privada em termos de maior **eficiência preditiva** e de **redução de danos** (BRAGA, 2016). Um sistema de câmeras de vigilância baseado em algoritmos de reconhecimento de padrões de comportamento, por exemplo, originado de *softwares*militares de vigilância de fronteiras, permite que a segurança privada identifique ameaças potenciais antes que elas se materializem em um evento criminoso, mudando o foco da resposta reativa para a prevenção proativa, o que representa um avanço significativo em relação aos métodos tradicionais de patrulhamento estático. É crucial ressaltar que essa transferência de tecnologias não se limita à compra de equipamentos já prontos, mas envolve a aquisição de **metodologias de gerenciamento** e **disciplina operacional** que são intrínsecas ao *modus operandi* militar, resultando em equipes de segurança privada mais bem treinadas em resposta a crises, em coordenação complexa e em emprego de força de forma escalonada, embora o uso efetivo da força letal continue sendo um tabu regulatório e legal no setor.

A interface entre a tecnologia militar e a segurança privada gera, contudo, um dilema de poder e legitimidade, pois a empresa privada, ao utilizar ferramentas desenvolvidas para o exercício da soberania estatal e para a defesa da nação, passa a emular capacidades de vigilância e coleta de informações que, em um Estado Democrático de Direito, deveriam estar estritamente sujeitas ao controle público e ao crivo judicial (FOUCAULT, 2014). A aquisição de *softwares* de *data fusion* (fusão de dados) por um banco ou uma mineradora, por exemplo, permite que a segurança corporativa cruze informações de múltiplas fontes, construindo perfis detalhados de indivíduos ou grupos de risco de forma que, se tal atividade fosse exercida pelo Estado, estaria sujeita a requisitos legais estritos, como a necessidade de mandado judicial ou de supervisão do Ministério Público, o que não ocorre na esfera privada, criando uma zona cinzenta de vigilância onde a privacidade do cidadão pode ser violada em nome da proteção do patrimônio (LEAL, 2018). Essa assimetria de controle público sobre as ferramentas de vigilância exige uma reflexão urgente sobre a necessidade de adaptar os princípios do Direito Público e Administrativo à crescente capacidade coercitiva e informacional do setor privado de segurança, para que a inovação tecnológica não se torne um catalisador da vigilância panóptica desregulamentada.

3. A Revolução dos Veículos Aéreos Não Tripulados (VANTs) na Segurança Privada

A incorporação dos Veículos Aéreos Não Tripulados, popularmente conhecidos como *drones*, representa, talvez, a mais visível e disruptiva inovação de origem militar a ser plenamente assimilada pelo setor de segurança privada no Brasil, alterando radicalmente as táticas de patrulhamento, monitoramento e resposta a incidentes em áreas extensas e de difícil acesso (OLIVEIRA, 2019). Desenvolvidos inicialmente para missões de reconhecimento, vigilância e aquisição de alvos (ISR - *Intelligence, Surveillance and Reconnaissance*) em teatros de guerra, os *drones* de uso comercial e civil adaptado oferecem à segurança patrimonial a capacidade de realizar o patrulhamento aéreo em tempo real, cobrindo grandes perímetros rurais, complexos

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

industriais, *campi* universitários ou áreas de *storage* logístico, com um custo operacional significativamente inferior ao patrulhamento com helicópteros ou aeronaves tripuladas, proporcionando uma eficiência de cobertura que era impensável há pouco mais de uma década e fornecendo uma perspectiva de monitoramento que supera as barreiras topográficas e as limitações do campo de visão humano.

Essa nova capacidade operacional permite que a segurança privada realize a inspeção remota de cercas, oleodutos e linhas de transmissão de energia, identificando intrusões ou falhas estruturais com precisão milimétrica, e, mais crucialmente, os VANTs podem ser empregados para o mapeamento e a vigilância de áreas de risco em situações de crise, como incêndios, desastres naturais ou invasões organizadas, fornecendo dados em alta resolução e em tempo hábil para a tomada de decisão da equipe de segurança em solo (SILVA, 2017). Tais equipamentos são frequentemente dotados de câmeras térmicas, sensores infravermelhos e sistemas de rastreamento por GPS de alta fidelidade, tecnologias que garantem a continuidade da vigilância mesmo sob condições adversas de luminosidade ou clima, conferindo à segurança privada um poder de observação que até recentemente era exclusividade de agências de inteligência e de forças armadas, o que exige um olhar cuidadoso do Direito sobre as implicações de seu uso desregulado, especialmente no que tange à captura indiscriminada de imagens e dados.

Do ponto de vista jurídico-regulatório, antes de 2020, o uso de *drones* no Brasil já estava sujeito às normativas da Agência Nacional de Aviação Civil (ANAC) e do Departamento de Controle do Espaço Aéreo (DECEA), órgãos de natureza militar e civil, respectivamente, que estabelecem regras rígidas sobre o registro das aeronaves, as áreas proibidas ou restritas para voo (incluindo proximidades de aeroportos e instalações militares) e a necessidade de autorização para operações não recreativas, o que impõe um regime de controle parcialmente eficaz sobre a navegação aérea, mas que se mostra insuficiente para lidar com as questões de invasão de privacidade e de coleta de dados pessoais (ANAC, 2017). Embora as regras da ANAC se concentrem na segurança do tráfego aéreo, elas não fornecem um arcabouço sólido para a responsabilização civil e criminal decorrente do uso indevido da capacidade de vigilância e de gravação dos VANTs, permitindo que a captação de imagens de propriedades vizinhas ou de áreas de descanso e lazer se torne uma prática comum sob o pretexto da segurança patrimonial, violando, de forma sistemática e tecnológica, a inviolabilidade da vida privada garantida constitucionalmente (BRASIL, 1988).

4. Sistemas de Monitoramento e *Softwares* de Inteligência Ciber-Militar

A transferência tecnológica dos sistemas de Comando e Controle (C2) e dos *softwares* de análise de inteligência desenvolvidos para fins militares representa um salto qualitativo ainda mais significativo para a segurança privada do que a mera introdução de *hardware* como os VANTs, pois estes sistemas conferem à segurança empresarial uma **capacidade cognitiva** de

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

processamento e interpretação de dados que mimetiza a *expertise* dos serviços de inteligência (GOMES, 2018). Tais *softwares*, originados de projetos de guerra assimétrica e de contraterrorismo, são capazes de realizar a fusão de dados (*data fusion*) provenientes de múltiplas fontes de vigilância, como câmeras de Circuito Fechado de Televisão (CFTV), sensores de acesso, dados de transações financeiras e até mesmo informações abertas coletadas na *internet* (OSINT - *Open Source Intelligence*), correlacionando-as em tempo real para identificar padrões, anomalias e ameaças potenciais antes que elas se manifestem em perdas patrimoniais ou operacionais.

A adaptação desses sistemas para o ambiente corporativo se manifesta em *softwares* de monitoramento que utilizam algoritmos de *Machine Learning* para criar "linhas de base" comportamentais, ou seja, modelos estatísticos do que é considerado um comportamento normal dentro de um determinado perímetro de segurança, e que disparam alertas automatizados quando um padrão divergente é detectado, como a permanência de um veículo em uma área restrita por tempo excessivo, a circulação de um indivíduo em um horário incomum ou a tentativa de acesso a um sistema por um usuário não autorizado (SOUZA, 2016). Essa capacidade preditiva, extraída da experiência militar em prever movimentos inimigos ou atividades de células terroristas, confere à segurança privada uma vantagem tática enorme, permitindo o acionamento de equipes de resposta com uma precisão e uma velocidade que os métodos de vigilância humana baseados em turnos e observação passiva jamais poderiam alcançar, resultando em uma drástica redução do tempo de resposta a incidentes críticos e, consequentemente, na minimização dos prejuízos.

Entretanto, é na aplicação desses *softwares* de inteligência que reside o mais grave dilema ético e jurídico, pois a eficácia preditiva desses sistemas depende da coleta e do processamento ininterrupto de um volume maciço de dados comportamentais de funcionários, clientes e terceiros que circulam pelas áreas sob vigilância, incluindo dados biométricos (reconhecimento facial), horários de entrada e saída e rotas de deslocamento (CASTELS, 2016). O uso de algoritmos de reconhecimento facial, que até o período anterior a 2020 não possuía uma regulamentação específica e robusta no Brasil (sendo a Lei Geral de Proteção de Dados - LGPD apenas sancionada em 2018), permite que a segurança privada construa perfis detalhados de indivíduos, extrapolando a mera proteção patrimonial para ingressar em uma esfera de vigilância comportamental de caráter quase panóptico, onde a vida privada e a liberdade de movimento do cidadão são monitoradas e catalogadas por entidades privadas que operam sem o devido controle democrático e a transparência exigida das agências de segurança pública (GIDDENS, 2019).

5. Técnicas de Inteligência e Contra-Inteligência de Origem Militar no Âmbito Corporativo

A transferência de *expertise* militar para a segurança privada não se limita a *hardware* e *software*, abrangendo também a incorporação de **metodologias de inteligência e contra-inteligência** que transformam a gestão de risco empresarial de uma atividade reativa para uma função estratégica e

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

proativa, passando a se denominar **Inteligência Corporativa**(PINHEIRO, 2017). Tais técnicas, originárias da doutrina militar de coleta, processamento e disseminação de informações para apoiar a decisão operacional em campo, são adaptadas para o ambiente corporativo com o objetivo de proteger ativos intangíveis (como segredos comerciais e *know-how*), prevenir fraudes internas, realizar a proteção executiva de alta *performance* e monitorar a reputação da empresa em ambientes de alto risco ou de competição acirrada, oferecendo um *framework* para a identificação de ameaças que o simples serviço de vigilância jamais conseguiria alcançar.

Uma das técnicas mais importantes transferidas é a **Inteligência de Fontes Abertas (*Open Source Intelligence* – OSINT)**, que, utilizada militarmente para monitorar grupos inimigos ou a situação política de nações instáveis por meio de informações disponíveis publicamente (redes sociais, notícias, *blogs*, *papers* acadêmicos), é aplicada no setor privado para realizar a *due diligence* de parceiros de negócios, monitorar a atividade de concorrentes ou identificar a formação de grupos de risco internos (como funcionários insatisfeitos ou grupos de ativistas que planejam ações contra a empresa), permitindo a intervenção preventiva da segurança antes que a ameaça se materialize (SANTOS, 2018). Essa metodologia exige a criação de células de inteligência dentro das corporações, compostas por analistas que utilizam a disciplina e o rigor metodológico da inteligência militar para transformar o volume de ruído informacional em dados acionáveis e preditivos, elevando a segurança a um nível estratégico de suporte à decisão executiva e à continuidade dos negócios.

No campo da **Contra-Inteligência**, o setor privado incorpora as técnicas militares para proteger-se de espionagem industrial, sabotagem e vazamento de informações confidenciais, aplicando metodologias de varredura eletrônica (TSCM - *Technical Surveillance Countermeasures*) e de análise de vulnerabilidade de redes, que visam neutralizar as tentativas de invasão ou monitoramento por parte de concorrentes ou agentes mal-intencionados (GARCIA, 2016). A transferência desse *know-how*, historicamente empregado na proteção de segredos de Estado e na segurança de chefes de governo, demonstra o quanto o risco corporativo é percebido como uma ameaça de "nível nacional" pela alta gestão, mas ao mesmo tempo levanta sérias questões sobre a invasão de esferas privadas e o monitoramento de funcionários, especialmente quando tais técnicas são utilizadas para investigar atividades sindicais ou para controlar a vida privada do colaborador fora do ambiente de trabalho, o que claramente ultrapassa a função de proteção patrimonial e ingressa na área de abuso de poder investigatório.

6. Implicações Jurídicas da Expansão Tecnológica na Segurança Privada

A rápida e desregulamentada adoção de tecnologias e metodologias de origem militar pelo setor de segurança privada cria um cenário de profundas implicações jurídicas no Brasil, especialmente no que tange ao equilíbrio constitucional entre a proteção do patrimônio (direito privado) e a garantia dos direitos fundamentais da cidadania (direito público), sendo o ponto focal o **limite do exercício do poder de vigilância e do uso da força por agentes privados** (VIEIRA, 2015). O

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

ordenamento jurídico brasileiro, anterior a 2020, possuía marcos regulatórios focados principalmente na vigilância ostensiva e no transporte de valores, delegando o controle da segurança tecnológica (drones, softwares de análise) a normas setoriais dispersas e insuficientes, como as já mencionadas da ANAC, que não se destinam primariamente à proteção da privacidade, resultando em um **vácuo normativo** onde o poder de coerção e a capacidade investigativa do setor privado floresceram.

O uso de VANTs e *softwares* de reconhecimento facial, que permitem a coleta de dados de forma massiva e a identificação precisa de indivíduos em tempo real, colide diretamente com a **inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas**, garantida pelo Artigo 5º, inciso X, da Constituição Federal, exigindo que o Direito Público estabeleça um marco de proporcionalidade entre o interesse do proprietário em proteger seu ativo e o direito do cidadão de não ser filmado, monitorado e catalogado de forma contínua e sem consentimento por entidades privadas (MORAES, 2014). Diferentemente da ação estatal, que só pode restringir direitos por meio de lei e mediante controle judicial (reserva de jurisdição), a vigilância privada opera sob a lógica da maximização do lucro e da minimização do risco, o que tende a levar à invasão de esferas privadas em nome da eficiência operacional, demandando uma intervenção legislativa urgente para definir parâmetros claros de uso, armazenamento e descarte dos dados coletados por esses aparatos de vigilância de alto poder.

Ademais, a aplicação de técnicas de inteligência e contra-inteligência militar em ambientes corporativos levanta a questão da **legalidade das investigações privadas** que se assemelham a inquéritos policiais ou atividades de órgãos de Estado, especialmente quando tais investigações extrapolam o ambiente físico da empresa para monitorar a vida privada de funcionários ou concorrentes (BRITO, 2018). Embora a Constituição assegure o direito à informação e o direito de propriedade, a atividade de Inteligência Corporativa não pode violar o sigilo de comunicações, a inviolabilidade de domicílio ou o sigilo bancário/fiscal, prerrogativas que exigem ordem judicial expressa e que são reservadas ao poder público. A ausência de regras específicas sobre o monitoramento de *e-mails* corporativos, a fiscalização de redes sociais e o uso de técnicas de *open source intelligence* (OSINT) pelos agentes privados confere-lhes um poder investigativo que carece de legitimidade democrática e controle social, exigindo que o Direito Administrativo e o Direito Penal estabeleçam limites claros para a atuação do setor e prevejam sanções severas para o desvio de finalidade na utilização de tecnologias de vigilância de origem militar.

7. Dilemas Éticos e a Desumanização do Serviço: O Impacto na Liberdade Civil

A crescente militarização tecnológica da segurança privada não é apenas um desafio jurídico-regulatório, mas, em sua essência, um complexo dilema ético que toca diretamente na **desumanização das relações sociais e no potencial erosivo sobre a liberdade civil e o direito**

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

à privacidade (BAUMAN, 2017). Ao depender cada vez mais de algoritmos preditivos, de sensores e de *drones* para a detecção de ameaças, o serviço de segurança tende a substituir o julgamento humano e a mediação interpessoal pela precisão fria da máquina e do código binário, resultando em uma vigilância que não distingue entre um comportamento atípico meramente inofensivo e uma ameaça criminosa real, tratando todos os indivíduos dentro do perímetro de vigilância como potenciais alvos de monitoramento e de desconfiança sistêmica.

O dilema da **vigilância massiva** é central, pois os *softwares* de análise de dados e de reconhecimento facial, desenvolvidos para fins militares de vigilância em larga escala, quando aplicados ao ambiente corporativo, criam uma cultura de escrutínio contínuo que pode inibir a liberdade de expressão, a atividade sindical e a própria espontaneidade das interações sociais nos locais de trabalho, em *shopping centers* ou em condomínios residenciais de alto padrão (HABERMAS, 2015). O cidadão passa a ser objeto de uma coleta de dados ininterrupta, onde suas rotinas, seus hábitos de consumo e suas interações são transformados em *inputs* para um sistema algorítmico de risco, sem que haja uma autorização clara, um propósito limitado ou um mecanismo transparente para a contestação dos dados, o que configura uma violação do direito à autodeterminação informativa e um desrespeito à dignidade humana, que exige o tratamento do indivíduo como fim, e não como mero meio de informação para a segurança patrimonial.

Adicionalmente, a dependência excessiva de tecnologias de origem militar para a segurança privada levanta a questão da **responsabilidade ética** em caso de falhas ou de uso abusivo do poder de vigilância. Se um *drone* equipado com *software* preditivo identifica erroneamente um indivíduo como potencial invasor, e este é abordado de forma violenta ou desproporcional por um agente de segurança terceirizado, a responsabilidade ética pela falha se dilui entre o fabricante do *software*, a empresa de segurança, o agente em campo e o cliente que contratou o serviço, dificultando a responsabilização civil e moral, o que evidencia a urgência na criação de códigos de ética específicos e na exigência de treinamento humanizado para os operadores dessas tecnologias (JONES, 2019). É imperativo que a ética na segurança privada, ao absorver o poder da tecnologia militar, priorize o respeito aos direitos humanos e às liberdades civis acima da mera proteção do lucro, reconhecendo que a segurança do patrimônio não pode ser dissociada da segurança da pessoa e de seus direitos fundamentais.

8. Conclusão Ampliada: Regulamentação Urgente e a Reafirmação da Supremacia do Direito Público

A investigação sobre a transposição de tecnologias e metodologias de origem militar para o setor de segurança privada revela um fenômeno de dupla face: por um lado, assiste-se a uma inegável e necessária elevação da eficiência na gestão de riscos e na prevenção de perdas em um contexto de ameaças complexas; por outro, constata-se a emergência de um desafio jurídico e ético de

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

proporções inéditas, onde o poder de vigilância, antes reservado ao Estado e sujeito a um rigoroso controle democrático, passa a ser exercido por entidades privadas, muitas vezes sem a devida transparência e sem o arcabouço normativo de proteção dos direitos fundamentais que é inerente ao Estado Democrático de Direito. A incorporação de VANTs, *softwares* de análise preditiva e técnicas de inteligência e contra-inteligência corporativa, embora se justifique pela lógica do mercado e da segurança patrimonial, coloca em risco o direito à privacidade, à imagem, à intimidade e, em última instância, à liberdade de ação do cidadão, exigindo uma resposta coordenada do Poder Público.

É inadiável a necessidade de intervenção do Poder Legislativo para a criação de um **marco regulatório específico e robusto** que defina os limites do poder de vigilância e de coleta de dados pelo setor de segurança privada, indo além das normativas de tráfego aéreo e das diretrizes genéricas de *data privacy* que, no contexto anterior a 2020, se mostravam insuficientes para lidar com o avanço da tecnologia de dupla utilização. Este novo arcabouço deve estabelecer, sob a ótica do Direito Público, princípios de estrita necessidade, proporcionalidade e finalidade na utilização dessas tecnologias, exigindo que a vigilância de alta capacidade seja restrita a áreas e períodos de risco comprovado, e que a coleta de dados biométricos e comportamentais seja realizada com o consentimento informado do indivíduo e sob a supervisão rigorosa de órgãos reguladores, garantindo a rastreabilidade e a prestação de contas dos agentes privados.

A dimensão ética, por sua vez, exige que a **civilidade** e a **dignidade humana** sejam reafirmadas como valores supremos que limitam a aplicação tecnológica, impedindo que a eficiência na proteção do patrimônio desumanize o serviço ou transforme o cidadão comum em mero objeto de vigilância panóptica. A solução para o dilema não reside na proibição da inovação, que é motor do desenvolvimento social e da própria segurança, mas sim na sua **regulação qualificada**, que assegure que a transferência do *know-how* militar para o setor privado seja feita de forma responsável e transparente, mantendo a supremacia do interesse público sobre o interesse privado na tutela dos direitos fundamentais. O Direito, portanto, deve agir como o guardião da Constituição, garantindo que o poder da tecnologia, mesmo que em mãos privadas, seja exercido dentro dos limites da lei e com o máximo respeito às liberdades civis, confirmando o monopólio da força e da coerção de alto nível como prerrogativa indelegável do Estado, sujeito ao escrutínio democrático.

Referências

ANAC. **Regulamento Brasileiro de Aviação Civil Especial RBAC-E nº 94: Requisitos Gerais para Aeronaves Não Tripuladas de Uso Civil**. Brasília, DF, 2017.

BAUMAN, Zygmunt. **Vigilância Líquida**. Rio de Janeiro: Zahar, 2017.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988.

BRAGA, Sérgio. **Segurança Corporativa: Estratégias e Tecnologias de Duplo Uso**. São Paulo: Érica, 2016.

BRITO, Francisco. **Investigação Empresarial e Limites Legais: O Direito à Privacidade do Empregado**. 3. ed. Rio de Janeiro: Lumen Juris, 2018.

CASTELS, Manuel. **A Galáxia da Internet: Reflexões sobre a Internet, os Negócios e a Sociedade**. Rio de Janeiro: Zahar, 2016.

FOUCAULT, Michel. **Vigiar e Punir: Nascimento da Prisão**. 42. ed. Petrópolis: Vozes, 2014.

GARCIA, Júlio C. **Contra-Inteligência Corporativa: Protegendo Ativos Intangíveis**. Curitiba: Juruá, 2016.

GIDDENS, Anthony. **Sociologia**. 6. ed. Porto Alegre: Artmed, 2019.

GOMES, André L. **Inteligência e Gestão de Riscos**. Rio de Janeiro: Elsevier, 2018.

HARTZ, Vera. **Saúde, Segurança e Ambiente em Empresas: A Gestão de Riscos**. 2. ed. São Paulo: Atlas, 2015.

JONES, Helen. **Ética em Vigilância e Tecnologia**. São Paulo: Perspectiva, 2019.

LEAL, Roberto A. **Direito à Privacidade na Era da Vigilância Tecnológica**. 4. ed. Belo Horizonte: Del Rey, 2018.

MORAES, Alexandre de. **Direito Constitucional**. 30. ed. São Paulo: Atlas, 2014.

OLIVEIRA, Lúcia R. **VANTs e a Nova Fronteira da Vigilância**. São Paulo: Editora USP, 2019.

PEREIRA, Carlos A. **Tecnologias de Duplo Uso e Segurança Internacional**. São Paulo: Fundação Getúlio Vargas, 2019.

PINHEIRO, Fernando S. **Inteligência Corporativa: A Visão Estratégica**. Rio de Janeiro: Qualitymark, 2017.

SANTOS, Boaventura de Sousa. **Pela Mão de Alice: O Social e o Político na Pós-Modernidade**. 14. ed. São Paulo: Cortez, 2017.

SANTOS, Ricardo. **OSINT: O Poder da Inteligência de Fontes Abertas**. 2. ed. Brasília: Editora IESB, 2018.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

SILVA, Eduardo N. **Segurança de Perímetros com Drones: Aspectos Técnicos e Legais**. Salvador: Juspodivm, 2017.

SOARES, Luiz Eduardo. **Segurança Pública: Estado e Sociedade Civil no Brasil**. 4. ed. Rio de Janeiro: Civilização Brasileira, 2018.

SOUZA, Marcos R. **Big Data na Segurança: Previsão e Prevenção de Risco**. Curitiba: InterSaberes, 2016.

TILLY, Charles. **As Relações Perigosas: Capital e Coerção na Formação dos Estados**. Rio de Janeiro: Paz e Terra, 1985.

VIEIRA, Oscar V. **O Direito e a Força na Segurança Privada**. São Paulo: Malheiros, 2015.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.