REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.4 out/dez. 2026 DOI: 10.47538/RA-2026.V5N4
ISSN: 2965-0003

A DUALIDADE DOS SISTEMAS DE AERONAVES NÃO TRIPULADAS NA SEGURANÇA PESSOAL PRIVADA: RISCOS LATENTES, VULNERABILIDADES LEGAIS E NOVOS PROTOCOLOS DE PROTEÇÃO

Sidney de Oliveira Carvalho
Especialista em Segurança Pública e Estratégia de Defesa pela Associação dos Diplomados da Escola Superior de Guerra (ADESG). https://orcid.org/0009-0000-8176-8756. E-mail: defenseact@hotmail.com

DOI-Geral: http://dx.doi.org/10.47538/RA-2026.V5N4
DOI-individual: http://dx.doi.org/10.47538/ra-2026.V5N4-20

RESUMO: Este artigo examina os efeitos da difusão dos sistemas de aeronaves não tripuladas (UAS), conhecidos como drones, sobre a segurança pessoal privada no Brasil. O objetivo é analisar como a mesma tecnologia que amplia a capacidade de observação das equipes de proteção executiva também favorece o reconhecimento de rotinas e os ataques praticados por organizações criminosas, e propor protocolos de prevenção compatíveis com o ordenamento jurídico vigente. Trata-se de pesquisa qualitativa e exploratória, de base bibliográfica e documental, que reuniu a legislação e as normas regulatórias em vigor em novembro de 2026, literatura técnica sobre detecção de drones e registros jornalísticos de eventos recentes. A análise mostra que a Resolução Anatel nº 760/2023 veda, em qualquer hipótese, o uso de bloqueadores de sinais por pessoas jurídicas de direito privado, enquanto o Estatuto da Segurança Privada (Lei nº 14.967/2024) não trata de aeronaves não tripuladas nem de contramedidas. No mesmo período, há registros do emprego de drones com explosivos por facção criminosa no Rio de Janeiro e da circulação ilegal de bloqueadores entre grupos criminosos. Conclui-se que, sem capacidade legal de neutralização ativa, a segurança privada precisa organizar sua resposta em torno da detecção passiva, da redução da previsibilidade, da proteção física das áreas críticas e da integração com os órgãos públicos legitimados a intervir.

PALAVRAS-CHAVE: Aeronaves não tripuladas. Segurança privada. Proteção executiva. Bloqueadores de sinal. Contramedidas antidrone.

THE DUALITY OF UNMANNED AIRCRAFT SYSTEMS IN PRIVATE PERSONAL SECURITY: LATENT RISKS, LEGAL VULNERABILITIES AND NEW PROTECTION PROTOCOLS

ABSTRACT: This article examines the effects of the spread of unmanned aircraft systems (UAS), commonly known as drones, on private personal security in Brazil. It analyzes how the same technology that expands the observation capacity of executive protection teams also supports routine reconnaissance and attacks by criminal organizations, and proposes prevention protocols compatible with the current legal framework. This is a qualitative, exploratory study based on bibliographic and documentary research, covering the legislation and regulations in force in November 2026, technical literature on drone detection and press records of recent events. The analysis shows that Anatel Resolution No. 760/2023 prohibits, under any circumstances, the use of signal jammers by private legal entities, while the Private Security Statute (Law

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.4 out/dez. 2026 DOI: 10.47538/RA-2026.V5N4
ISSN: 2965-0003

No. 14,967/2024) does not address unmanned aircraft or countermeasures. Over the same period, there are records of drones carrying explosives being used by a criminal faction in Rio de Janeiro and of jammers circulating illegally among criminal groups. The study concludes that, lacking legal capacity for active neutralization, private security must structure its response around passive detection, reduced predictability, physical protection of critical areas and integration with the public agencies legally entitled to intervene.

KEYWORDS: Unmanned aircraft. Private security. Executive protection. Signal jammers. Counter-drone measures.

INTRODUÇÃO

A popularização das aeronaves não tripuladas de uso comercial alterou, em poucos anos, a relação entre quem protege e quem observa. Equipamentos vendidos livremente, com câmeras de alta resolução, sensores térmicos e estabilização automática, passaram a oferecer a qualquer operador uma perspectiva aérea que, até pouco tempo, dependia de helicópteros ou de estruturas fixas.

Para as equipes de segurança pessoal, isso representa um recurso de reconhecimento de rotas, de vigilância de perímetros e de documentação de ocorrências. Para quem pretende atingir uma pessoa protegida, a mesma tecnologia permite observar hábitos, contar vigilantes, mapear acessos e, em situações extremas, transportar cargas nocivas até o alvo.

No Brasil, a segurança pessoal é uma das atividades de segurança privada reconhecidas pelo Estatuto da Segurança Privada e da Segurança das Instituições Financeiras, instituído pela Lei nº 14.967, de 9 de setembro de 2024. O art. 5º, inciso IX, define o serviço como a "execução de segurança pessoal com a finalidade de preservar a integridade física de pessoas", e o art. 4º condiciona a prestação dos serviços à autorização prévia da Polícia Federal, a quem cabem o controle e a fiscalização da atividade (Brasil, 2024). O texto do Estatuto, porém, não menciona aeronaves não tripuladas, seja como ferramenta à disposição das equipes, seja como ameaça a ser enfrentada.

A questão ganha relevo porque as regras que incidem sobre o tema foram produzidas por órgãos diferentes e com finalidades diferentes. A Agência Nacional de Telecomunicações (Anatel) disciplina o uso do espectro e, com ele, os bloqueadores de

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.4 out/dez. 2026 DOI: 10.47538/RA-2026.V5N4
ISSN: 2965-0003

sinais. A Agência Nacional de Aviação Civil (ANAC) e o Departamento de Controle do Espaço Aéreo (DECEA) regulam o cadastro, a operação e o acesso das aeronaves ao espaço aéreo. A Polícia Federal autoriza e fiscaliza as empresas de segurança. Nenhum desses conjuntos normativos foi pensado para responder à pergunta prática que se coloca à equipe de um guarda-costas quando um drone desconhecido se aproxima da residência do protegido.

O presente estudo parte da seguinte pergunta: como as equipes de segurança pessoal privada podem reduzir a exposição de seus protegidos às ameaças originadas de drones, considerando que o ordenamento brasileiro lhes nega o uso de bloqueadores de sinais? O objetivo geral é analisar essa dupla condição da tecnologia, ao mesmo tempo instrumento de proteção e vetor de ameaça, e propor protocolos de prevenção compatíveis com a legislação em vigor.

Os objetivos específicos são: (a) descrever as aplicações defensivas dos drones na proteção executiva e as condições regulatórias de seu uso; (b) caracterizar, a partir de registros recentes, o emprego de drones por organizações criminosas no país; (c) examinar o regime jurídico dos bloqueadores de sinais e os limites da neutralização física por particulares; e (d) sistematizar medidas preventivas que não dependam de emissão de radiofrequência nem de intervenção cinética.

Nas fontes reunidas para esta pesquisa, as discussões sobre contramedidas a drones concentram-se em instalações militares, aeroportos, estabelecimentos prisionais e infraestruturas críticas. Não se localizou, nesse levantamento, estudo dedicado especificamente à proteção de pessoas pela segurança privada brasileira diante do novo quadro regulatório de 2023 a 2026, o que justifica a abordagem aqui adotada. Após esta introdução, a seção 2 descreve o método; a seção 3 trata do uso defensivo dos drones; a seção 4, da ameaça criminosa; a seção 5, do regime dos bloqueadores e da neutralização física; a seção 6 apresenta os protocolos propostos; a seção 7 discute implicações e limitações; e a seção 8 reúne as considerações finais.

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.4 out/dez. 2026 DOI: 10.47538/RA-2026.V5N4
ISSN: 2965-0003

METODOLOGIA

Trata-se de pesquisa qualitativa, de caráter exploratório, conduzida por meio de levantamento bibliográfico e documental. O caráter exploratório decorre da novidade do problema: o marco regulatório dos drones foi substituído em 2026, o regulamento dos bloqueadores de sinais foi renovado em 2023 e o Estatuto da Segurança Privada entrou em vigor em 2024, de modo que ainda não há acúmulo de estudos que articulem essas normas no campo da proteção de pessoas.

O corpus foi organizado em três grupos. O primeiro reúne as normas jurídicas e regulatórias: a Constituição Federal de 1988, o Código Penal, a Lei Geral de Telecomunicações (Lei nº 9.472/1997), a Lei nº 9.296/1996, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), a Lei nº 14.967/2024, a Resolução Anatel nº 760/2023, a Resolução ANAC nº 805/2026, que aprovou o RBAC nº 100, e a Instrução do Comando da Aeronáutica ICA 100-40, na versão aprovada em março de 2026.

O segundo grupo compreende literatura técnica sobre detecção de aeronaves não tripuladas e sobre o enquadramento jurídico das contramedidas, com destaque para Kaleem e Rehmani (2018), Taha e Shoufan (2019) e Dieckert (2021). O terceiro grupo é formado por registros jornalísticos de 2025 e 2026 sobre o uso de drones e de bloqueadores por grupos criminosos no Brasil.

As buscas foram realizadas em novembro de 2026, em portais oficiais de legislação, em páginas institucionais dos órgãos reguladores e em bases de indexação científica. A análise seguiu três eixos definidos a partir da pergunta de pesquisa: a capacidade defensiva que a tecnologia oferece às equipes de proteção; a natureza e a evolução da ameaça; e os limites legais impostos à atuação de particulares. As propostas da seção 6 resultam do cruzamento desses eixos e devem ser lidas como hipóteses de trabalho a serem testadas em campo, e não como resultados empíricos.

Os registros jornalísticos foram utilizados apenas como evidência de ocorrência dos fatos e não como fonte estatística. Essa cautela se justifica pela própria variação dos números divulgados: na operação policial de outubro de 2025 no Rio de Janeiro, mencionada na seção 4, as primeiras edições noticiaram ao menos 64 mortos, ao passo

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.4 out/dez. 2026 DOI: 10.47538/RA-2026.V5N4
ISSN: 2965-0003

que reportagem publicada três dias depois já mencionava 121 (Drones..., 2025; Vale, 2025). O estudo não envolveu coleta de dados com seres humanos e, por isso, não foi submetido a Comitê de Ética em Pesquisa.

O EMPREGO DEFENSIVO DOS DRONES NA PROTEÇÃO EXECUTIVA

GANHOS OPERACIONAIS

Para uma equipe de segurança pessoal, a principal contribuição do drone é a altura. Um observador aéreo enxerga, de uma só vez, o que uma equipe terrestre levaria vários minutos para percorrer: as vias de acesso a um local de evento, os pontos em que um comboio é obrigado a reduzir a velocidade, os veículos estacionados próximos à residência do protegido e os imóveis com visada direta sobre áreas de embarque e desembarque. Equipamentos com câmera térmica estendem essa observação ao período noturno e permitem identificar pessoas ocultas por vegetação ou sombra.

Esse recurso pode ser aplicado em três momentos. Antes do deslocamento, serve para o reconhecimento de rotas alternativas e para a verificação de obstruções, obras ou aglomerações. Durante eventos, permite acompanhar o perímetro externo e orientar o posicionamento dos agentes em solo. Depois de uma ocorrência, as imagens registradas auxiliam a reconstrução dos fatos e a comunicação às autoridades. Em todos os casos, o drone complementa a equipe terrestre e não a substitui, porque a resposta a qualquer ameaça continua a depender de pessoas posicionadas junto ao protegido.

Há também usos menos evidentes. A observação aérea periódica da própria residência do cliente, feita pela equipe de segurança, ajuda a identificar o que um observador hostil enxergaria: pátios expostos, horários em que a família permanece em áreas abertas, janelas sem anteparo visual e trajetos internos previsíveis. Essa leitura do imóvel a partir de cima é a base de várias medidas propostas na seção 6.

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.4 out/dez. 2026 DOI: 10.47538/RA-2026.V5N4
ISSN: 2965-0003

CONDICIONANTES REGULATÓRIAS DO USO DEFENSIVO

O uso de drones pelas equipes de proteção está sujeito às mesmas regras aplicáveis a qualquer operador civil. Em 15 de junho de 2026, a ANAC aprovou, por meio da Resolução nº 805, o Regulamento Brasileiro da Aviação Civil nº 100 (RBAC nº 100), que substituiu integralmente o RBAC-E nº 94. O novo regulamento organiza as operações nas categorias aberta, específica e certificada, define responsabilidades do operador e do piloto remoto e exige que toda aeronave não tripulada seja cadastrada na ANAC e vinculada a uma pessoa física ou jurídica com CPF ou CNPJ no Brasil. O cadastro tem validade de 24 meses e prevê isenção, em certas condições, para aeronaves de até 250 gramas (Brasil, 2026a).

No plano do espaço aéreo, a nova versão da ICA 100-40, aprovada pela Portaria DECEA nº 2094/DNOR8, de 18 de março de 2026, com vigência a partir de 1º de julho de 2026, passou a exigir autorização prévia pelo sistema SARPAS para os voos de drones no país, incluindo os equipamentos com peso máximo de decolagem inferior a 250 gramas, que antes tinham tratamento diferenciado (Brasil, 2026b). Para a segurança privada, isso significa que o uso do drone precisa ser planejado com antecedência e integrado à rotina documental da empresa. O voo improvisado, motivado por uma suspeita no momento, encontra limites regulatórios que a equipe deve conhecer antes de decolar.

O Estatuto da Segurança Privada não proíbe nem disciplina especificamente o uso de drones. Seu art. 2º faz referência ao emprego de "tecnologias e equipamentos de uso permitido" (Brasil, 2024), o que sugere que a ferramenta pode ser incorporada aos serviços desde que observadas as normas da aviação civil e do espaço aéreo. Essa leitura é uma interpretação deste estudo e depende de confirmação pela regulamentação do Estatuto e pela prática fiscalizatória da Polícia Federal.

Há, por fim, a questão da privacidade. A captação de imagens em áreas urbanas alcança vizinhos, transeuntes e funcionários, o que atrai a incidência da Lei Geral de Proteção de Dados Pessoais. Os princípios da finalidade, da adequação e da necessidade, previstos no art. 6º dessa lei (Brasil, 2018), recomendam que a empresa defina por escrito

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.4 out/dez. 2026 DOI: 10.47538/RA-2026.V5N4
ISSN: 2965-0003

para que as imagens são captadas, por quanto tempo são guardadas e quem tem acesso a elas.

A ASSIMETRIA DA AMEAÇA: O USO POR ORGANIZAÇÕES CRIMINOSAS

RECONHECIMENTO E VIGILÂNCIA

O mesmo recurso que orienta a equipe de proteção serve a quem planeja um ataque. Em reportagem de 31 de outubro de 2025, baseada em denúncia do Ministério Público do Estado do Rio de Janeiro, foram divulgadas conversas em que integrantes do Comando Vermelho discutiam a necessidade de adquirir drones com visão noturna e térmica para vigiar a movimentação policial à noite. Um dos investigados afirma que o grupo "tem que se adequar à tecnologia", e outro observa que a câmera de que dispunha mostrava apenas escuridão no período noturno (Vale, 2025). O episódio indica que o reconhecimento aéreo já integra o planejamento de grupos criminosos estruturados.

Transposto para a proteção de pessoas, esse tipo de capacidade permite levantar, sem aproximação física, o padrão de vida do protegido e de sua família: horários de saída e chegada, veículos utilizados, número de agentes, momentos de troca de turno, disposição de portões, garagens e áreas de lazer. Essa transposição é uma inferência analítica deste trabalho e não um dado observado em casos concretos de segurança privada, mas decorre diretamente das capacidades descritas nos registros mencionados.

LOGÍSTICA ILÍCITA E DOMÍNIO OPERACIONAL

O emprego de drones para levar celulares, drogas e outros objetos a unidades prisionais mostra que os grupos criminosos dominam não apenas a observação, mas também o transporte de cargas com precisão. Em outubro de 2026, o secretário da Administração Penitenciária e Ressocialização do Ceará, Mauro Albuquerque, afirmou que os presídios do estado chegaram a sofrer, em média, 30 investidas de drones por dia entre 2021 e 2026, com pico em 2024 e 2025, e que o número caiu para cerca de uma por semana. Segundo o secretário, 38 drones foram abatidos e 29 pilotos foram presos desde

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.4 out/dez. 2026 DOI: 10.47538/RA-2026.V5N4
ISSN: 2965-0003

o período de maior incidência (Delivery..., 2026). O próprio secretário não apresentou dados detalhados, o que reforça a necessidade de tratar esses números como indicação de escala, e não como estatística consolidada.

AMEAÇA CINÉTICA

A passagem do reconhecimento ao ataque ficou documentada em 28 de outubro de 2025, durante a Operação Contenção, realizada nos complexos da Penha e do Alemão, no Rio de Janeiro. Segundo a cobertura da imprensa, integrantes do Comando Vermelho utilizaram drones para lançar granadas contra os agentes, em uma reação que durou mais de doze horas, e o fato foi apontado como inédito na segurança pública fluminense (Drones..., 2025). O alvo, naquele caso, eram forças policiais em operação. O registro importa para a segurança privada porque demonstra que a adaptação de drones comerciais para o lançamento de explosivos já está ao alcance de organizações criminosas que atuam em áreas urbanas brasileiras.

IDENTIFICAÇÃO E RASTREABILIDADE

É comum a afirmação de que os drones operam sem qualquer sistema de identificação obrigatória. No caso brasileiro, essa afirmação precisa ser qualificada. O RBAC nº 100 exige o cadastro das aeronaves com vinculação a CPF ou CNPJ (Brasil, 2026a), e a ICA 100-40 exige autorização prévia para os voos (Brasil, 2026b). Esses instrumentos, contudo, dependem da adesão do próprio operador. Quem pretende usar o equipamento para fins ilícitos simplesmente não o cadastra nem solicita autorização.

Nos Estados Unidos, a Federal Aviation Administration adotou a regra de identificação remota (Remote ID), codificada na Parte 89 do Título 14 do Código de Regulamentos Federais, cuja exigência passou a ser fiscalizada a partir de 16 de março de 2024. A agência descreve o mecanismo como uma espécie de placa digital que permite às autoridades localizar a estação de controle quando um drone voa de forma insegura ou em área proibida (Federal Aviation Administration, 2023).

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.4 out/dez. 2026 DOI: 10.47538/RA-2026.V5N4
ISSN: 2965-0003

Nas normas brasileiras examinadas nesta pesquisa, não se identificou obrigação equivalente de transmissão de identificação em voo. Ainda que viesse a existir, operadores hostis poderiam recorrer a equipamentos montados artesanalmente ou modificados para não transmitir, de modo que a identificação remota ajudaria sobretudo a separar os voos regulares dos suspeitos, sem eliminar a ameaça.

O PARADOXO REGULATÓRIO: BLOQUEADORES DE SINAIS E NEUTRALIZAÇÃO FÍSICA

O REGIME DOS BLOQUEADORES DE SINAIS

Os bloqueadores de sinais de radiocomunicações (BSR), conhecidos como *jammers*, costumam ser descritos como equipamentos restritos às atividades de segurança pública, defesa nacional e estabelecimentos prisionais. Essa descrição corresponde, em linhas gerais, ao regime da Resolução Anatel nº 308/2002, que foi substituída pela Resolução nº 760, de 6 de fevereiro de 2023. O regulamento atual ampliou os usos admitidos, mas manteve, de forma ainda mais explícita, a exclusão dos particulares.

Pelo art. 2º da Resolução nº 760/2023, são vedados em todo o país a comercialização, a posse e o emprego de BSR, salvo nas circunstâncias excepcionais previstas no regulamento e mediante anuência da Anatel. O art. 4º enumera os órgãos da Administração Pública que podem atuar como usuários, entre eles a Presidência da República, o Gabinete de Segurança Institucional, os Ministérios da Defesa, da Justiça e Segurança Pública e das Relações Exteriores, as Forças Armadas, a Agência Brasileira de Inteligência, os órgãos de segurança pública e os órgãos de administração penitenciária.

O art. 6º limita o uso a determinadas áreas de bloqueio: estabelecimentos penitenciários, portos e aeroportos, áreas de segurança pública ou militares e locais temporários de interesse de órgãos de segurança pública, de defesa nacional e de delegações estrangeiras. Quanto aos particulares, o art. 5º, § 1º, é categórico: “Em hipótese alguma a Anatel anuirá ao uso de BSR por pessoa natural ou por pessoa jurídica de direito privado” (Brasil, 2023).

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.4 out/dez. 2026 DOI: 10.47538/RA-2026.V5N4
ISSN: 2965-0003

Ao justificar a ampliação do regulamento, a própria Anatel apontou que o equipamento pode ser indispensável para a contenção de drones, além de grandes eventos e da proteção de sistemas críticos baseados em navegação por satélite (Anatel..., 2023). O Estado, portanto, reconhece o bloqueador como ferramenta antidrone, mas o reserva aos seus próprios órgãos. Empresas de segurança privada, como pessoas jurídicas de direito privado, estão alcançadas pela vedação, ainda que o regulamento não as mencione pelo nome.

CONSEQUÊNCIAS DO USO NÃO AUTORIZADO

Além das sanções administrativas, o emprego de bloqueador sem autorização pode, em tese, atrair a incidência do art. 183 da Lei nº 9.472/1997, que tipifica a conduta de "desenvolver clandestinamente atividades de telecomunicação", com pena de detenção de dois a quatro anos, aumentada da metade se houver dano a terceiro, e multa (Brasil, 1997). O enquadramento específico do uso de bloqueadores nesse tipo penal é uma questão de interpretação que este estudo não pretende resolver, mas o risco jurídico é suficiente para afastar a hipótese de uso pela segurança privada.

Há também razões técnicas para cautela. O bloqueio atinge indistintamente as comunicações móveis, a navegação por satélite e outros serviços na área afetada, inclusive os da própria equipe de proteção e os de serviços de emergência. Além disso, sua eficácia é limitada. Dieckert (2021) observa que o bloqueio só funciona se o drone estiver sendo pilotado remotamente ou navegando por GPS, e não contra voos pré-programados. Ou seja, mesmo que fosse permitido, o bloqueador não ofereceria proteção completa contra um ataque planejado.

A ASSIMETRIA EM RELAÇÃO AOS GRUPOS CRIMINOSOS

Enquanto as empresas autorizadas estão impedidas de operar bloqueadores, os grupos criminosos os adquirem no mercado ilegal. Em setembro de 2025, foi preso em Sorocaba, São Paulo, um homem apontado como um dos principais fornecedores de equipamentos eletrônicos para facções do Rio de Janeiro. Segundo a reportagem, ele

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.4 out/dez. 2026 DOI: 10.47538/RA-2026.V5N4
ISSN: 2965-0003

fornecia bloqueadores capazes de interferir em sinais de celulares, drones e GPS, utilizados para dificultar a atuação das forças de segurança e facilitar sequestros, roubos e o controle de territórios (Polícia..., 2025). O quadro é de assimetria: o agressor dispõe, ilegalmente, de um recurso que o defensor regular não pode usar. É importante registrar, porém, que essa assimetria não resulta de uma falha isolada da norma, e sim da opção legítima de reservar ao Estado uma tecnologia que produz efeitos sobre terceiros.

NEUTRALIZAÇÃO FÍSICA E LEGÍTIMA DEFESA

Afastado o bloqueio, resta a hipótese de neutralização física: derrubar o drone por disparo, por rede lançada ou por colisão com outro drone. O ordenamento não prevê essa atuação para a segurança privada. A Constituição atribui a segurança pública ao Estado (art. 144), e o Estatuto da Segurança Privada proíbe o uso de produtos controlados de uso restrito na prestação dos serviços, salvo nos casos definidos em regulamento (Brasil, 1988; Brasil, 2024, art. 11). Resta a legítima defesa, prevista no art. 25 do Código Penal para quem, "usando moderadamente dos meios necessários, repele injusta agressão, atual ou iminente, a direito seu ou de outrem" (Brasil, 1940).

A experiência europeia, analisada por Dieckert (2021), ajuda a dimensionar o problema. O autor admite que um drone que se aproxima sem justificativa pode, em certas circunstâncias, ser tratado como agressão em curso, o que justificaria medidas enérgicas. Ressalva, porém, que o ônus da prova recai sobre quem se defende e conclui que as empresas devem evitar defesas desse tipo enquanto não houver marco legal que as autorize expressamente. A essa ressalva jurídica soma-se o risco material: a queda de um drone sobre área urbana pode ferir terceiros, e o disparo contra um objeto em voo expõe pessoas que nada têm a ver com a ameaça. Por essas razões, a neutralização física não deve integrar a rotina das equipes privadas. A legítima defesa permanece como resposta excepcional, sujeita a exame posterior das circunstâncias.

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.4 out/dez. 2026 DOI: 10.47538/RA-2026.V5N4
ISSN: 2965-0003

DETECÇÃO COMO ESPAÇO LEGÍTIMO DE ATUAÇÃO

O mesmo autor faz uma distinção útil entre mitigação e detecção. Segundo Dieckert (2021), os sistemas que apenas recebem sinais, sem emitir transmissões próprias, podem ser operados por particulares na maioria dos Estados europeus, com as devidas cautelas de proteção de dados. A mitigação, por sua vez, permanece reservada às autoridades. O regime brasileiro segue lógica semelhante, já que a Resolução nº 760/2023 trata de equipamentos que emitem sinais para interferir em comunicações. Detectar não é bloquear. É nesse espaço, o da percepção antecipada e da reação organizada, que a segurança privada pode atuar com segurança jurídica.

PROPOSTA DE PROTOCOLOS DE PREVENÇÃO

Diante da impossibilidade legal de neutralização ativa, propõe-se que as equipes de segurança pessoal organizem sua resposta em cinco eixos. O quinto eixo decorre diretamente da análise normativa da seção 5. As medidas são apresentadas como propostas, cuja eficácia depende de avaliação em campo.

DETECÇÃO PASSIVA MULTISSENSORIAL

A detecção passiva combina sensores que captam sinais emitidos pelo próprio drone ou pelo ambiente, sem transmitir nada. Os principais são os sensores acústicos, que reconhecem o som característico de motores e hélices; as câmeras ópticas e térmicas associadas a algoritmos de análise de imagem; e os receptores de radiofrequência, que identificam a presença de enlaces de controle e de vídeo. Taha e Shoufan (2019) revisaram a literatura sobre detecção e classificação de drones por aprendizado de máquina e apontam a combinação de diferentes modalidades como caminho para aumentar a confiabilidade.

O alcance desses sensores, porém, é bem menor do que se costuma supor. A literatura consultada não sustenta a ideia de identificação a quilômetros de distância com sensores passivos de uso viável em ambiente residencial. Kaleem e Rehmani (2018)

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.4 out/dez. 2026 DOI: 10.47538/RA-2026.V5N4
ISSN: 2965-0003

estimam alcance de 50 a 300 metros para a detecção acústica e de 50 a 400 metros para a detecção por câmeras ópticas e térmicas. Os mesmos autores apontam que ambientes ruidosos dificultam a separação do som do drone e que ruídos semelhantes, como o de veículos, podem gerar falsos alarmes. Registram ainda que o radar convencional tem desempenho limitado contra drones pequenos de plástico, que refletem pouco sinal.

Em termos operacionais, isso significa que a detecção passiva oferece um aviso de segundos a poucos minutos, e não de horas. O valor do sistema, portanto, depende do que a equipe faz com esse aviso. Cada alerta deve corresponder a uma ação previamente treinada, como recolher o protegido a um ambiente coberto, interromper um embarque ou alterar o trajeto. Sem essa vinculação, o sensor se torna apenas um registro do que aconteceu.

Dois cuidados jurídicos acompanham essa medida. O primeiro é limitar o monitoramento de radiofrequência à detecção da presença, da direção e do tipo de emissão, sem decodificar o conteúdo transmitido, para evitar conflito com o art. 10 da Lei nº 9.296/1996, que tipifica a interceptação de comunicações telemáticas sem autorização judicial (Brasil, 1996). O segundo é tratar as imagens captadas pelas câmeras de vigilância do espaço aéreo segundo as regras da LGPD, já mencionadas na seção 3.2.

REDUÇÃO DA PREVISIBILIDADE

O drone de reconhecimento é mais útil a quem o opera quando o alvo segue padrões. Por isso, a variação planejada de horários, trajetos, veículos e pontos de entrada e saída reduz o valor da vigilância aérea, porque o que foi observado em um dia deixa de servir para prever o dia seguinte. Propõe-se que essa variação seja planejada por meio de matrizes de alternativas definidas pela equipe, sorteadas ou combinadas de forma que nem mesmo os funcionários do protegido conheçam a rotina com muita antecedência.

A medida deve alcançar também a exposição voluntária de informações. Publicações em redes sociais com fotos da residência, da escola dos filhos ou de locais frequentados permitem ao observador hostil direcionar o voo com precisão,

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.4 out/dez. 2026 DOI: 10.47538/RA-2026.V5N4
ISSN: 2965-0003

economizando tempo de reconhecimento. Orientar o protegido e sua família sobre esse ponto é parte do mesmo esforço de reduzir a previsibilidade.

PROTEÇÃO FÍSICA E OCULTAÇÃO VISUAL

Como a detecção oferece pouco tempo de reação, as áreas em que o protegido fica mais exposto devem ser preparadas com antecedência. As principais são os pontos de embarque e desembarque, os pátios, as áreas de lazer e os acessos de pedestres. Propõe-se priorizar garagens cobertas e acessos que permitam ao protegido entrar e sair do veículo sem céu aberto sobre si; instalar telas tensionadas sobre pátios e áreas de lazer, capazes de reter ou desviar objetos lançados; usar coberturas e anteparos visuais em janelas e áreas de circulação observáveis do alto; e reduzir ao mínimo o tempo de permanência em áreas descobertas durante deslocamentos.

Quanto à ocultação contra sensores térmicos, há materiais que reduzem a assinatura de calor de pessoas e veículos, mas sua eficácia depende do tipo de material, da distância e da sensibilidade do equipamento utilizado pelo observador. Antes de incorporar esse recurso ao protocolo, recomenda-se testá-lo com câmeras térmicas comerciais equivalentes às disponíveis no mercado. A instalação de telas e coberturas, por sua vez, está sujeita às normas urbanísticas municipais e às regras condominiais aplicáveis.

VARREDURA ELETRÔNICA REVERSA

Analisadores de espectro operados de forma passiva podem indicar se a residência do protegido ou o trajeto da equipe está sendo acompanhado por um drone em voo controlado remotamente, a partir da presença de enlaces de controle e de transmissão de vídeo nas faixas de uso não licenciado comumente empregadas por drones comerciais, como 2,4 GHz e 5,8 GHz. A varredura periódica permite construir um perfil normal do ambiente eletromagnético do local e identificar alterações.

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.4 out/dez. 2026 DOI: 10.47538/RA-2026.V5N4
ISSN: 2965-0003

Essa medida tem limitação importante: drones que voam por rota pré-programada e sem transmissão de vídeo em tempo real emitem pouco ou nenhum sinal, o que os torna invisíveis à varredura de radiofrequência. Por isso, a varredura eletrônica deve ser combinada com os sensores acústicos e ópticos descritos no item 6.1, e não utilizada isoladamente.

INTEGRAÇÃO INSTITUCIONAL E PROTOCOLO DE RESPOSTA

Se a neutralização é prerrogativa do Estado, a segurança privada precisa de um caminho rápido para acionar quem pode exercê-la. Propõe-se que cada empresa estabeleça, para seus protegidos de maior risco, um protocolo escrito com a seguinte sequência: detecção e confirmação visual; recolhimento imediato do protegido a ambiente coberto; registro do horário, da direção, da altitude aproximada e de imagens do drone e, se possível, da posição provável do operador; comunicação imediata ao órgão de segurança pública competente; e comunicação posterior do voo irregular às autoridades aeronáuticas.

Para eventos de grande exposição, a Resolução Anatel nº 760/2023 admite o uso de bloqueadores pelos órgãos de segurança pública em locais temporários de seu interesse (Brasil, 2023, art. 6º). A coordenação prévia com esses órgãos, quando o evento justificar, é a forma legal de contar com capacidade de bloqueio sem que a empresa privada a opere. Por fim, o registro detalhado de cada ocorrência serve também à defesa da própria equipe, caso alguma medida tomada em situação de urgência venha a ser examinada posteriormente sob a ótica da legítima defesa.

O Quadro 1 resume as medidas discutidas, sua função e a situação legal para a segurança privada segundo a análise deste estudo.

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.4 out/dez. 2026 DOI: 10.47538/RA-2026.V5N4
ISSN: 2965-0003

Quadro 1: Medidas antidrone e sua situação legal para a segurança pessoal privada.

Medida	Função	Situação para a segurança privada	Principais limitações
Detecção acústica	Alerta pela assinatura sonora de motores e hélices	Admissível; não emite sinais	Alcance de dezenas a centenas de metros; falsos alarmes em ambiente ruidoso
Detecção óptica e térmica com análise de imagem	Alerta, classificação e registro visual	Admissível, com observância da LGPD	Alcance limitado; sensível a iluminação e condições climáticas
Monitoramento passivo de radiofrequência	Identificação de enlaces de controle e vídeo	Admissível se limitado à detecção, sem decodificar conteúdo	Não percebe drones em rota pré-programada sem transmissão
Redução da previsibilidade	Retirar valor do reconhecimento aéreo	Sem restrição legal	Custo logístico; exige disciplina do protegido e da família
Barreiras físicas e ocultação	Proteger áreas de maior exposição	Admissível, sujeita a normas urbanísticas e condominiais	Eficácia de materiais térmicos depende de teste
Acionamento de órgãos públicos	Viabilizar neutralização por quem tem competência	Recomendável; bloqueio por órgão público previsto no art. 6º da Res. 760/2023	Tempo de resposta; depende de coordenação prévia
Bloqueador de sinais	Interromper controle e navegação do drone	Vedado (Res. Anatel 760/2023, art. 5º, § 1º)	Afeta terceiros; ineficaz contra voos pré-programados
Neutralização física	Derrubar ou capturar o drone	Sem previsão legal; apenas legítima defesa excepcional	Risco a terceiros; ônus de justificar a medida

Fonte: Elaborado pelo autor com base em Brasil (2018, 2023, 2024), Kaleem e Rehmani (2018) e Dieckert (2021).

DISCUSSÃO E LIMITAÇÕES

A análise responde à pergunta de pesquisa em dois níveis. No nível operacional, a segurança pessoal privada pode reduzir a exposição de seus protegidos sem recorrer a bloqueadores, desde que aceite uma mudança de postura: em vez de buscar a interrupção do voo hostil, deve concentrar-se em percebê-lo cedo, em tornar o protegido menos previsível, em reduzir as áreas em que ele fica exposto e em acionar rapidamente quem tem competência para neutralizar a aeronave. No nível normativo, a vedação aos bloqueadores não é uma anomalia brasileira. O padrão descrito por Dieckert (2021) para a Europa é semelhante, com a detecção aberta aos particulares e a mitigação reservada às autoridades.

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.4 out/dez. 2026 DOI: 10.47538/RA-2026.V5N4
ISSN: 2965-0003

O ponto frágil do sistema brasileiro, segundo este estudo, não é a proibição em si, mas a ausência de canais específicos entre a segurança privada e os órgãos públicos para situações de ameaça aérea. O Estatuto da Segurança Privada é recente e silencia sobre drones. Sua regulamentação e os cursos de formação dos profissionais de segurança pessoal poderiam incorporar o tema, incluindo a operação regular de drones pelas equipes, a detecção passiva e os protocolos de resposta.

Dieckert (2021) menciona, para o contexto europeu, a proposta de conceder a operadores de infraestruturas críticas permissões específicas para medidas defensivas em cenários bem definidos. Uma discussão análoga poderia ser aberta no Brasil, com controle pela Polícia Federal e anuência da Anatel, embora isso dependa de alteração normativa e não seja objeto de proposta concreta neste trabalho.

O estudo tem limitações que precisam ser consideradas. Por ser bibliográfico e documental, não testou em campo nenhuma das medidas propostas, e os alcances de detecção citados vêm da literatura internacional, não de ensaios em ambiente urbano brasileiro. Os registros jornalísticos permitem afirmar que os fatos ocorreram, mas não oferecem base estatística, como mostra a variação dos números divulgados sobre a operação de outubro de 2025. As interpretações jurídicas apresentadas, especialmente quanto ao art. 183 da Lei Geral de Telecomunicações e ao alcance do art. 2º do Estatuto da Segurança Privada, não foram confrontadas com jurisprudência específica. Além disso, o RBAC nº 100 e a nova ICA 100-40 são de 2026 e ainda estão em fase de transição, o que pode alterar parte das condições descritas.

Como agenda de pesquisa, sugerem-se ensaios de detecção acústica e óptica em condomínios e vias urbanas brasileiras, com medição de alcance e de taxa de falsos alarmes; levantamento junto a empresas de segurança privada sobre incidentes envolvendo drones e sobre as práticas já adotadas; e estudo jurídico sobre a responsabilidade civil e penal de agentes privados que adotem medidas físicas contra drones em situações de urgência.

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.4 out/dez. 2026 DOI: 10.47538/RA-2026.V5N4
ISSN: 2965-0003

CONSIDERAÇÕES FINAIS

Os drones ampliaram a capacidade de observação das equipes de segurança pessoal e, ao mesmo tempo, colocaram ao alcance de grupos criminosos um instrumento de reconhecimento e de ataque que já foi usado no país. Diante dessa dupla condição, o ordenamento brasileiro reserva ao Estado os meios de neutralização ativa e veda aos particulares, em qualquer hipótese, o uso de bloqueadores de sinais.

Essa restrição não deixa a segurança privada sem resposta, mas define o tipo de resposta possível. A proteção passa a depender da detecção passiva, da redução da previsibilidade das rotinas, da preparação física das áreas de maior exposição e de protocolos que liguem o alerta à ação imediata da equipe e ao acionamento das autoridades. A incorporação desses elementos à regulamentação do Estatuto da Segurança Privada e à formação dos profissionais de segurança pessoal permitiria que o setor acompanhasse uma ameaça que já não é hipotética.

REFERÊNCIAS

ANATEL. Amplia uso de bloqueadores de sinais para além dos presídios. **Minha Operadora**, [*s. l.*], [2023]. Disponível em: https://www.minhaoperadora.com.br/?p=111092. Acesso em: 4 nov. 2026.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 4 nov. 2026.

BRASIL. Agência Nacional de Aviação Civil. Resolução nº 805, de 15 de junho de 2026. Aprova o RBAC nº 100, e emendas aos RBACs nºs 90 e 137, e altera a Resolução nº 659, de 2 de fevereiro de 2022. **Diário Oficial da União**, Brasília, DF, 16 jun. 2026a. Disponível em: https://pergamum.anac.gov.br/arquivos/RA2026-0805.pdf. Acesso em: 4 nov. 2026.

BRASIL. Agência Nacional de Telecomunicações. Resolução nº 760, de 6 de fevereiro de 2023. Aprova o Regulamento sobre Bloqueador de Sinais de Radiocomunicações. **Diário Oficial da União**, Brasília, DF, 8 fev. 2023. Disponível em: https://www.normasbrasil.com.br/norma/resolucao-760-2023_442215.html. Acesso em: 4 nov. 2026.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. **ICA 100-40**: aeronaves não tripuladas e o acesso ao espaço aéreo brasileiro. Aprovada pela Portaria DECEA nº 2094/DNOR8, de 18 de março de 2026. Rio de Janeiro: DECEA, 2026b. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/aerolevantamento/

REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.4 out/dez. 2026 DOI: 10.47538/RA-2026.V5N4
ISSN: 2965-0003

arquivos/2026/ica-100-40_18_03_2026_-01_07_2026-vigencia.pdf. Acesso em: 4 nov. 2026.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. **Diário Oficial da União**, Rio de Janeiro, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 4 nov. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 4 nov. 2026.

BRASIL. Lei nº 14.967, de 9 de setembro de 2024. Institui o Estatuto da Segurança Privada e da Segurança das Instituições Financeiras. **Diário Oficial da União**, Brasília, DF, 10 set. 2024. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/lei/l14967.htm. Acesso em: 4 nov. 2026.

BRASIL. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. **Diário Oficial da União**, Brasília, DF, 25 jul. 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 4 nov. 2026.

BRASIL. Lei nº 9.472, de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995. **Diário Oficial da União**, Brasília, DF, 17 jul. 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9472.htm. Acesso em: 4 nov. 2026.

DELIVERY do crime: presídios cearenses sofriam 30 ataques de drone por dia, diz secretário. **Diário do Nordeste**, Fortaleza, 14 out. 2026. Disponível em: https://diariodonordeste.verdesmares.com.br/seguranca/delivery-do-crime-presidios-cearenses-sofriam-30-ataques-de-drone-por-dia-diz-secretario-1.3798623. Acesso em: 4 nov. 2026.

DIECKERT, Ulrich. Regulatory frameworks in support of counter-UAS. *In*: JOINT AIR POWER COMPETENCE CENTRE. **A comprehensive approach to countering unmanned aircraft systems**. Kalkar: JAPCC, 2021. Disponível em: https://www.japcc.org/chapters/c-uas-regulatory-frameworks-in-support-of-counter-uas/. Acesso em: 4 nov. 2026.

DRONES com explosivo, bloqueios em série, alta letalidade: o que megaoperação no Rio teve de inédito. **Folha de Pernambuco**, Recife, 29 out. 2025. Conteúdo da Agência O Globo. Disponível em: https://www.folhape.com.br/noticias/drones-com-explosivo-bloqueios-em-serie-alta-letalidade-o-que/446914/. Acesso em: 4 nov. 2026.

FEDERAL AVIATION ADMINISTRATION. **FAA extends Remote ID enforcement date six months**. Washington, DC: FAA, 13 set. 2023. Disponível em: https://www.faa.gov/newsroom/faa-extends-remote-id-enforcement-date-six-months. Acesso em: 4 nov. 2026.



REVISTA ELETRÔNICA AMPLAMENTE
v.5, n.4 out/dez. 2026 DOI: 10.47538/RA-2026.V5N4
ISSN: 2965-0003

KALEEM, Zeeshan; REHMANI, Mubashir Husain. Amateur drone monitoring: state-of-the-art architectures, key enabling technologies, and future research directions. **IEEE Wireless Communications**, [*s. l.*], v. 25, n. 2, p. 150-159, abr. 2018. DOI: 10.1109/MWC.2018.1700152.

POLÍCIA prende em Sorocaba fornecedor de bloqueadores de sinais usados por facções do Rio. **Lex Legal**, [*s. l.*], 14 set. 2025. Disponível em: https://lexlegal.com.br/?p=36162. Acesso em: 4 nov. 2026.

TAHA, Bilal; SHOUFAN, Abdulhadi. Machine learning-based drone detection and classification: state-of-the-art in research. **IEEE Access**, [*s. l.*], v. 7, p. 138669-138682, 2019. DOI: 10.1109/ACCESS.2019.2942944.

VALE, Caroline. Facção planejou comprar drone noturno para vigiar polícia no Rio: "a gente tem que se adequar à tecnologia". **SBT News**, [*s. l.*], 31 out. 2025. Disponível em: https://sbtnews.sbt.com.br/noticia/brasil/faccao-comprou-drone-noturno-para-vigiar-policia-no-rio-a-gente-tem-que-se-adequar-a-tecnologia. Acesso em: 4 nov. 2026.

Submissão: julho de 2026. Aceite: agosto de 2026. Publicação: outubro de 2026.