RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.
Year II, v.2 2022. | Submission: 11/11/2022 | Accepted: 13/11/2022 | Publication: 15/11/2022

Military Technologies in Private Security: Innovations and APPLICATIONS

MILITARY TECHNOLOGIES IN PRIVATE SECURITY: INNOVATIONS AND APPLICATIONS

Author: Rodrigo Hipólito Menezes de Araújo.

Graduated in Law from ULBRA - Lutheran University of Brazil.

Postgraduate student in Public Law at the University of Amazonas - UEA

Summary

This scientific article aims to investigate the phenomenon of the transposition and adaptation of technologies and methodologies of military origin to 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 the context of corporate risk management. The central objective is to demonstrate how such innovations increase efficiency in threat prevention and response, while simultaneously raising complex ethical dilemmas related to mass surveillance and the preservation of fundamental guarantees of citizenship. It concludes with the urgent need to update the national regulatory framework to reconcile technological innovation with the imperatives of the Democratic Rule of Law, especially regarding privacy and the limits of the exercise of private police power.

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

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

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. Introduction: Technological Transposition and the Blurred Boundary between Public and Private

Security, in its sociological and legal conception, represents one of the most elementary social demands and one of the primary duties of the State, establishing the legitimate monopoly of force as the mainstay of public order and social peace; however, the inability or insufficiency of state action to fully meet this demand, especially in contexts of high urban complexity and escalating organized crime, has engendered an exponential growth of the private security sector, which historically was limited to low-cost, visible, and property surveillance with reduced technological incorporation (SOARES, 2018).

This growth, observed globally since the end of the 20th century, has been accompanied by a qualitative transformation in the nature of the services provided, driven by a market dynamic that demands high efficiency, predictive precision, and, above all, the minimization of risks inherent to the activity. This has culminated in the search for *know-how* and equipment historically restricted to the domain of defense and high-performance military operations , thus characterizing a process of silent and technologically mediated militarization. This technological and methodological transposition from the spheres of security and defense to the corporate and private sector cannot be analyzed merely as operational optimization or a business *marketing* strategy , but rather as a socio-political phenomenon that destabilizes the classic distinction between the apparatus of public coercion and asset protection activities, requiring a critical reassessment of the limits of surveillance power and the legal implications of this transfer of *expertise* and adapted military equipment.

The core of this investigation lies in the detailed analysis of how dual-use resources, originally developed and improved in military theaters of operations and strategic intelligence environments, are adapted and incorporated by private security companies to address increasingly sophisticated threats, such as the theft of high-value cargo, the intrusion of *data centers ,* or the protection of large critical infrastructures, which demand solutions that far exceed the operational capacity of conventional human security (TILLY, 1985). This includes the incorporation of *drones* (UAVs) for perimeter patrol and the use of predictive analytics *software* based on facial or pattern recognition algorithms.

Behavioral technologies, which in turn find their roots in military command and control systems, are paradigmatic examples of this technological symbiosis that redefines the security landscape. The central problem, therefore, does not lie in the legality of the technology itself, but in the absence of a normative framework that can keep pace with the speed of innovation, generating a regulatory vacuum where the power of private surveillance can be exercised without due social control and without the effective safeguarding of citizens' rights to privacy, intimacy, and image, as advocated by the 1988 Federal Constitution (BRAZIL, 1988).

It is therefore imperative that academia and Public Law examine the nature and consequences of this technological absorption, understanding that efficiency in reducing risks for the private sector cannot be achieved at the cost of undermining the protection of fundamental rights. This analysis is conducted with methodological rigor that seeks to balance the description of operational innovations with the legal and ethical critique inherent to the subject (SANTOS, 2017). The structure of this article is designed to examine, in its subsequent chapters, the technological and methodological instruments transferred, the legal implications of their application, and finally, the ethical dilemmas that this expansion of surveillance and data collection capacity imposes on civil society and on the very concept of security as a public good, culminating in a broader reflection on the need for urgent and specific regulation.

2. The Technological Paradigm and the Military-Private Convergence in Risk Management

The concept of **dual-use technologies** serves as the main theoretical vector for understanding the rapid absorption of military *hardware* and *software* by the private security sector. These technologies are characterized by their applicability in both military or national defense contexts and in civilian or commercial applications, facilitating the migration of knowledge and equipment developed with public military research funds to the open security market (PEREIRA, 2019). This process is not accidental, but rather a reflection of the restructuring of the military-industrial complex after the Cold War, a period in which there was a demobilization of *expertise* and a surplus of technologies that, in order to find a new market, were simplified, reduced in cost, and adapted to meet the growing demand for protection in a globalized corporate environment, where operational, logistical, and reputational risks became a priority for large business conglomerates and owners of critical infrastructure (HARTZ, 2015). This convergence is evident in areas such as remote sensing, robotics, and big data analytics , fields where massive military investment has resulted in monitoring and surveillance tools with unparalleled precision.

The logic driving this absorption lies fundamentally in the technical superiority and reliability of military and defense equipment, designed to operate under extreme conditions and to perform target detection and tracking with a minimal margin of error.

These characteristics translate to private security in terms of greater **predictive efficiency** and **damage reduction** (BRAGA, 2016). A surveillance camera system based on behavioral pattern recognition algorithms, for example, originating from military border surveillance software, allows private security to identify potential threats before they materialize into a criminal event, shifting the focus from reactive response to proactive prevention, which represents a significant advance over traditional static patrolling methods. It is crucial to emphasize that this technology transfer is not limited to the purchase of ready-made equipment, but involves the acquisition of **management methodologies** and **operational discipline** that are intrinsic to the *modus operandi.*

military training has resulted in private security teams being better trained in crisis response, complex coordination, and the use of force in a phased manner, although the effective use of lethal force remains a regulatory and legal taboo in the sector.

The interface between military technology and private security, however, generates a dilemma of power and legitimacy, since the private company, by using tools developed for the exercise of state sovereignty and for the defense of the nation, begins to emulate surveillance and information gathering capabilities that, in a democratic state governed by the rule of law, should be strictly subject to public control and judicial scrutiny (FOUCAULT, 2014). The acquisition of *data* fusion *software* (Data merging) by a bank or a mining company, for example, allows corporate security to cross-reference information from multiple sources, building detailed profiles of individuals or at-risk groups in such a way that, if such activity were carried out by the State, it would be subject to strict legal requirements, such as the need for a court order or supervision by the Public Prosecutor's Office, which does not occur in the private sphere, creating a gray area of surveillance where the citizen's privacy can be violated in the name of protecting property (LEAL, 2018). This asymmetry of public control over surveillance tools demands an urgent reflection on the need to adapt the principles of Public and Administrative Law to the growing coercive and informational capacity of the private security sector, so that technological innovation does not become a catalyst for unregulated panoptic surveillance.

3. The Revolution of Unmanned Aerial Vehicles (UAVs) in Private Security

The incorporation of Unmanned Aerial Vehicles, popularly known as *drones,* represents perhaps the most visible and disruptive innovation of military origin to be fully assimilated by the private security sector in Brazil, radically altering patrolling, monitoring, and incident response tactics in extensive and difficult-to-access areas (OLIVEIRA, 2019). Initially developed for intelligence, surveillance, and target acquisition (ISR) missions in war theaters, commercially and civilian *drones* offer property security the ability to perform real-time aerial patrols, covering large rural perimeters and complexes.

Industrial areas, university *campuses ,* or logistics *storage* areas , with a significantly lower operating cost than patrolling with helicopters or manned aircraft, providing coverage efficiency that was unthinkable just over a decade ago and offering a monitoring perspective that overcomes topographical barriers and the limitations of the human field of vision.

This new operational capability allows private security to remotely inspect fences, pipelines, and power transmission lines, identifying intrusions or structural flaws with millimeter precision. More crucially, UAVs can be used for mapping and surveillance of high-risk areas in crisis situations, such as fires, natural disasters, or organized invasions, providing high-resolution data in a timely manner for decision-making by the security team on the ground (SILVA, 2017). Such equipment is frequently equipped with thermal cameras, infrared sensors, and high-fidelity GPS tracking systems, technologies that ensure continuous surveillance even under adverse lighting or weather conditions. This gives private security an observational power that until recently was the exclusive domain of intelligence agencies and armed forces, requiring careful legal consideration of the implications of its unregulated use, especially regarding the indiscriminate capture of images and data.

From a legal and regulatory standpoint, prior to 2020, the use of *drones* in Brazil was already subject to the regulations of the National Civil Aviation Agency (ANAC) and the Department of Airspace Control (DECEA), military and civilian bodies, respectively, which establish strict rules on aircraft registration, prohibited or restricted flight areas (including the vicinity of airports and military installations), and the need for authorization for non-recreational operations. This imposes a partially effective control regime over air navigation, but one that proves insufficient to address issues of privacy invasion and the collection of personal data (ANAC, 2017). Although ANAC's rules focus on air traffic safety, they do not provide a solid framework for civil and criminal liability arising from the misuse of the surveillance and recording capabilities of UAVs, allowing the capture of images of neighboring properties or rest and leisure areas to become a common practice under the pretext of property security, systematically and technologically violating the constitutionally guaranteed inviolability of private life (BRAZIL, 1988).

4. Monitoring Systems and Cyber-Military Intelligence *Software*

The technological transfer of Command and Control (C2) systems and intelligence analysis *software* developed for military purposes represents an even more significant qualitative leap for private security than the mere introduction of *hardware* such as UAVs, as these systems provide corporate security with a **cognitive capability** of

Data processing and interpretation that mimics the *expertise* of intelligence services (GOMES, 2018). Such *software,* originating from asymmetric warfare and counterterrorism projects, is capable of performing data fusion *from* multiple surveillance sources, such as Closed Circuit Television (CCTV) cameras, access sensors, financial transaction data, and even open information collected on the *internet* (OSINT).
Open Source Intelligence), correlating them in real time to identify patterns, anomalies, and potential threats before they manifest as asset or operational losses.

The adaptation of these systems to the corporate environment manifests itself in monitoring *software* that uses *Machine Learning* algorithms to create behavioral "baselines," that is, statistical models of what is considered normal behavior within a given security perimeter, and that trigger automated alerts when a divergent pattern is detected, such as a vehicle remaining in a restricted area for an excessive amount of time, an individual circulating at an unusual time, or an unauthorized user attempting to access a system (SOUZA, 2016). This predictive capacity, drawn from military experience in predicting enemy movements or terrorist cell activities, gives private security a huge tactical advantage, allowing the activation of response teams with a precision and speed that human surveillance methods based on shifts and passive observation could never achieve, resulting in a drastic reduction in response time to critical incidents and, consequently, in minimizing losses.

However, the most serious ethical and legal dilemma lies in the application of these intelligence *software programs ,* since the predictive effectiveness of these systems depends on the uninterrupted collection and processing of a massive volume of behavioral data from employees, clients, and third parties circulating in the areas under surveillance, including biometric data (facial recognition), entry and exit times, and travel routes (CASTELS, 2016). The use of facial recognition algorithms, which until the period prior to 2020 lacked specific and robust regulation in Brazil (the General Data Protection Law - LGPD - was only sanctioned in 2018), allows private security to build detailed profiles of individuals, going beyond mere property protection to enter a sphere of behavioral surveillance of an almost panoptic nature, where the private life and freedom of movement of citizens are monitored and cataloged by private entities operating without due democratic control and...
Transparency required of public safety agencies (GIDDENS, 2019).

5. Intelligence and Counter-Intelligence Techniques of Military Origin in the Corporate Sphere

The transfer of military *expertise* to private security is not limited to *hardware* and *software;* it also encompasses the incorporation of **intelligence and counter-intelligence methodologies** that transform corporate risk management from a reactive activity into a strategic function.

Proactive, and now called **Corporate Intelligence (PINHEIRO,** 2017). These techniques, originating from the military doctrine of collecting, processing, and disseminating information to support operational decision-making in the field, are adapted to the corporate environment with the aim of protecting intangible assets (such as trade secrets and *know-how),* preventing internal fraud, providing high- *performance* executive protection , and monitoring the company's reputation in high-risk or highly competitive environments, offering a *framework* for identifying threats that simple surveillance services could never achieve.

One of the most important techniques transferred is **Open Source Intelligence *(OSINT),*** which, used militarily to monitor enemy groups or the political situation of unstable nations through publicly available information (social networks, news, *blogs,* academic *papers),* is applied in the private sector to conduct *due diligence* on business partners, monitor competitor activity, or identify the formation of internal risk groups (such as disgruntled employees or activist groups planning actions against the company), allowing for preventive security intervention before the threat materializes (SANTOS, 2018). This methodology requires the creation of intelligence cells within corporations, composed of analysts who use the discipline and methodological rigor of military intelligence to transform the volume of informational noise into actionable and predictive data, elevating security to a strategic level of support for executive decision-making and business continuity.

In the field of **Counterintelligence,** the private sector incorporates military techniques to protect itself from industrial espionage, sabotage, and leaks of confidential information, applying electronic surveillance methodologies (TSCM - *Technical Surveillance Countermeasures)* and network vulnerability analysis, which aim to neutralize attempts at intrusion or monitoring by competitors or malicious agents (GARCIA, 2016). The transfer of this *know-how,* historically employed in the protection of state secrets and the security of heads of government, demonstrates how corporate risk is perceived as a "national level" threat by senior management, but at the same time raises serious questions about the invasion of private spheres and the monitoring of employees, especially when such techniques are used to investigate union activities or to control the employee's private life outside the workplace, which clearly goes beyond the function of asset protection and enters the area of abuse of investigative power.

6. Legal Implications of Technological Expansion in Private Security

The rapid and unregulated adoption of technologies and methodologies of military origin by the private security sector creates a scenario with profound legal implications in Brazil, especially regarding the constitutional balance between the protection of property (private law) and the guarantee of fundamental rights of citizenship (public law), with the focal point being the **limit of the exercise of surveillance power and the use of force by private agents** (VIEIRA

Prior to 2020, the Brazilian legal system had regulatory frameworks focused primarily on overt surveillance and the transportation of valuables, delegating control of technological security (drones, analysis software) to scattered and insufficient sectoral regulations, such as those already mentioned from ANAC (National Civil Aviation Agency), which are not primarily intended to protect privacy, resulting in a **regulatory vacuum** where the coercive power and investigative capacity of the private sector flourished.

The use of UAVs and facial recognition *software ,* which allow for the massive collection of data and the precise identification of individuals in real time, directly clashes with the **inviolability of privacy, private life, honor, and image of individuals,** guaranteed by Article 5, item X, of the Federal Constitution. This requires Public Law to establish a framework of proportionality between the owner's interest in protecting their asset and the citizen's right not to be filmed, monitored, and cataloged continuously and without consent by private entities (MORAES, 2014). Unlike state action, which can only restrict rights through law and under judicial control (jurisdictional reservation), private surveillance operates under the logic of profit maximization and risk minimization, which tends to lead to the invasion of private spheres in the name of operational efficiency. This demands urgent legislative intervention to define clear parameters for the use, storage, and disposal of data collected by these high-powered surveillance devices.

Furthermore, the application of military intelligence and counter-intelligence techniques in corporate environments raises the question of the **legality of private investigations** that resemble police inquiries or activities of state bodies, especially when such investigations extend beyond the physical environment of the company to monitor the private lives of employees or competitors (BRITO, 2018). Although the Constitution guarantees the right to information and the right to property, Corporate Intelligence activity cannot violate the secrecy of communications, the inviolability of domicile, or banking/tax secrecy, prerogatives that require an express court order and are reserved for the public authorities. The absence of specific rules on the monitoring of corporate *emails ,* the surveillance of social networks, and the use of *open source intelligence* (OSINT) techniques by private agents grants them an investigative power that lacks democratic legitimacy and social control, requiring that Administrative Law and Criminal Law establish clear limits for the sector's activities and provide for severe sanctions for the misuse of surveillance technologies of military origin.

7. Ethical Dilemmas and the Dehumanization of Service: The Impact on Civil Liberties

The increasing technological militarization of private security is not merely a legal and regulatory challenge, but, in essence, a complex ethical dilemma that directly touches upon the **dehumanization of social relations and its erosive potential on civil liberties and the law.**

to privacy (BAUMAN, 2017). By increasingly relying on predictive algorithms, sensors, and *drones* for threat detection, security services tend to replace human judgment and interpersonal mediation with the cold precision of machines and binary code, resulting in surveillance that does not distinguish between merely harmless atypical behavior and a real criminal threat, treating all individuals within the surveillance perimeter as potential targets of monitoring and systemic distrust.

The dilemma of **mass surveillance** is central, as data analysis and facial recognition *software ,* developed for large-scale military surveillance purposes, when applied to the corporate environment, create a culture of continuous scrutiny that can inhibit freedom of expression, union activity, and the very spontaneity of social interactions in workplaces, *shopping malls ,* or high-end residential condominiums (HABERMAS, 2015). Citizens become the object of uninterrupted data collection, where their routines, consumption habits, and interactions are transformed into *inputs* for an algorithmic risk system, without clear authorization, a limited purpose, or a transparent mechanism for contesting the data. This constitutes a violation of the right to informational self-determination and a disrespect for human dignity, which demands that the individual be treated as an end in itself, and not merely as a means of information for property security.

Additionally, the excessive reliance on military-derived technologies for private security raises the question of **ethical responsibility** in cases of failures or abuse of surveillance power. If a *drone* equipped with predictive *software* mistakenly identifies an individual as a potential intruder, and this individual is approached violently or disproportionately by a third-party security agent, ethical responsibility for the failure becomes diluted among the software manufacturer , the security company, the field agent, and the client who contracted the service, hindering civil and moral accountability. This highlights the urgency of creating specific codes of ethics and requiring humanized training for operators of these technologies (JONES, 2019). It is imperative that ethics in private security, when absorbing the power of military technology, prioritize respect for human rights and civil liberties above the mere protection of profit, recognizing that the security of property cannot be dissociated from the security of the person and their fundamental rights.

8. Expanded Conclusion: Urgent Regulation and the Reaffirmation of the Supremacy of Public Law

Research into the transfer of technologies and methodologies of military origin to the private security sector reveals a two-sided phenomenon: on the one hand, there is an undeniable and necessary increase in efficiency in risk management and loss prevention in a context of complex threats; on the other hand, there is an emerging legal and ethical challenge.

Unprecedented proportions, where the power of surveillance, previously reserved for the State and subject to rigorous democratic control, is now exercised by private entities, often without due transparency and without the normative framework for the protection of fundamental rights that is inherent to a democratic state governed by the rule of law. The incorporation of UAVs, predictive analytics *software ,* and corporate intelligence and counter-intelligence techniques, while justified by market logic and asset security, jeopardizes the right to privacy, image, intimacy, and ultimately, the freedom of action of citizens, requiring a coordinated response from the Public Authorities.

It is imperative that the Legislative Branch intervene to create a **specific and robust regulatory framework** that defines the limits of surveillance and data collection powers by the private security sector, going beyond air traffic regulations and generic *data privacy* guidelines which, in the pre-2020 context, proved insufficient to deal with the advancement of dual-use technology. This new framework must establish, from a Public Law perspective, principles of strict necessity, proportionality, and purpose in the use of these technologies, requiring that high-capacity surveillance be restricted to areas and periods of proven risk, and that the collection of biometric and behavioral data be carried out with the informed consent of the individual and under the rigorous supervision of regulatory bodies, guaranteeing the traceability and accountability of private agents.

The ethical dimension, in turn, demands that **civility** and **human dignity** be reaffirmed as supreme values that limit technological application, preventing efficiency in protecting property from dehumanizing the service or transforming the ordinary citizen into a mere object of panoptic surveillance. The solution to the dilemma does not lie in prohibiting innovation, which is the engine of social development and security itself, but rather in its **qualified regulation,** ensuring that the transfer of military *know-how* to the private sector is done responsibly and transparently, maintaining the supremacy of the public interest over the private interest in the protection of fundamental rights. The law, therefore, must act as the guardian of the Constitution, guaranteeing that the power of technology, even in private hands, is exercised within the limits of the law and with the utmost respect for civil liberties, confirming the monopoly of force and high-level coercion as an indelegable prerogative of the State, subject to democratic scrutiny.

References

ANAC. **Brazilian Civil Aviation Regulation RBAC-E No. 94: General Requirements for Unmanned Aircraft for Civil Use.** Brasília, DF, 2017.

BAUMAN, Zygmunt. **Liquid Surveillance.** Rio de Janeiro: Zahar, 2017.

BRAZIL. **Constitution of the Federative Republic of Brazil.** Brasília, DF: Federal Senate, 1988.

BRAGA, Sérgio. **Corporate Security: Dual-Use Strategies and Technologies.** São Paulo: Érica, 2016.

BRITO, Francisco. **Business Investigation and Legal Limits: The Employee's Right to Privacy.** 3rd ed. Rio de Janeiro: Lumen Juris, 2018.

CASTELS, Manuel. **The Internet Galaxy: Reflections on the Internet, Business, and Society.** Rio de Janeiro: Zahar, 2016.

FOUCAULT, Michel. **Discipline and Punish: The Birth of the Prison.** 42nd ed. Petrópolis: Vozes, 2014.

GARCIA, Júlio C. **Corporate Counterintelligence: Protecting Intangible Assets.** Curitiba: Juruá, 2016.

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

GOMES, André L. **Intelligence and Risk Management.** Rio de Janeiro: Elsevier, 2018.

HARTZ, Vera. **Health, Safety and Environment in Companies: Risk Management.** 2nd ed. São Paulo: Atlas, 2015.

JONES, Helen. **Ethics in Surveillance and Technology.** São Paulo: Perspectiva, 2019.

LEAL, Roberto A. **The Right to Privacy in the Age of Technological Surveillance.** 4th ed. Belo Horizonte: Del Rey, 2018.

MORAES, Alexandre de. **Constitutional Law.** 30th ed. São Paulo: Atlas, 2014.

OLIVEIRA, Lúcia R. **UAVs and the New Frontier of Surveillance.** São Paulo: Editora USP, 2019.

PEREIRA, Carlos A. **Dual-Use Technologies and International Security.** São Paulo: Fundação Getúlio Vargas, 2019.

PINHEIRO, Fernando S. **Corporate Intelligence: The Strategic Vision.** Rio de Janeiro: Qualitymark, 2017.

SANTOS, Boaventura de Sousa. **By the Hand of Alice: The Social and the Political in Post-Modernity.** 14th ed. São Paulo: Cortez, 2017.

SANTOS, Ricardo. **OSINT: The Power of Open Source Intelligence.** 2nd ed. Brasília: IESB Publishing House, 2018.

SILVA, Eduardo N. **Perimeter Security with Drones: Technical and Legal Aspects.** Salvador: Juspodivm, 2017.

SOARES, Luiz Eduardo. **Public Security: State and Civil Society in Brazil.** 4th ed. Rio de Janeiro: Civilização Brasileira, 2018.

SOUZA, Marcos R. **Big Data in Security: Risk Prediction and Prevention.** Curitiba: InterSaberes, 2016.

TILLY, Charles. **Dangerous Liaisons: Capital and Coercion in the Formation of States.** Rio de Janeiro: Paz e Terra, 1985.

VIEIRA, Oscar V. **Law and Force in Private Security.** São Paulo: Malheiros, 2015.