v. 4, n. 16, 2024

International Journal of Human Sciences Research

PREDICTIVE POLICE PROACTIVE ACTIONS AGAINST EXTREME VIOLENCE: STRENGTHENING POLICE INTELLIGENCE - THE BRAZILIAN CASE

Sergio Fernandes Senna Pires
Doctor of Psychology
Chamber of Deputies of Brazil

Abstract: This study delves into the vital importance of enhancing police intelligence to effectively counteract extreme violence, underscoring the necessity for advanced predictive measures against severe threats like terrorism, election interference, and school violence. We draw a clear distinction between predictive policing and proactive police strategies. We analyze the critical need for police specialization, embracing new technologies, and bolstering intelligence resources to preemptively tackle violence, while navigating the ethical and legal quandaries presented. We stress the imperative of maintaining a balance between ensuring public safety and upholding privacy rights, in compliance with Brazil's General Data Protection Law. The discussion extends to the risks of algorithmic bias in policing and it points out the need for independent audits and judicial oversight on surveillance tech use, and calls for legislative updates to keep pace with evolving security challenges. Highlighting the significance of continual professional development, adherence to ethical norms, fostering a security tech industry, and enhancing international cybersecurity cooperation. This study also posits that there is an urgent need for the modernization of laws concerning criminal organizations and the production of evidence. It argues for a comprehensive overhaul of existing legislation to include cutting-edge methodologies that can adapt to the complexities of contemporary crime dynamics. Additionally, this research underscores the importance of utilizing war game simulations, which allow for the testing of complex scenarios in controlled environments. Such simulations can indicate essential requirements for legislative modernization in this area, providing lawmakers with empirical data to craft more effective and responsive legal frameworks. These strategic simulations not only forecast potential challenges but also offer a robust platform for evaluating the implications of new laws before their enactment, thereby ensuring that legislative updates are both practical and well-informed. We conclude that an extensive dialogue is crucial for crafting a legislative framework that effectively combats extreme violence, anchored in solid scientific and technological support.
Keywords: terrorism; police intelligence; extreme violence; predictive police proactive actions.

INTRODUCTION

In the contemporary landscape, the ever-evolving threats to public safety underscore the growing significance of police intelligence within the context of preventative measures. Considering this, we aim to present theoretical elements, analyze, and discuss the essential needs for strengthening police intelligence activities, especially in combating extreme violence. Our focus particularly includes the use of prediction in police proactive actions, specifically targeting cybercrimes that result in extreme violence, such as terrorism; disinformation; manipulation of the democratic electoral process; hate group formation; and coordinated school attacks. In these instances, there's a pressing need for public safety forces to anticipate and predict potential violent events from their preparatory acts.

For a successful argument, it's crucial to differentiate between predictive police proactive actions and predictive policing, the latter being extensively debated in scholarly literature (Mugari & Obioha, 2021; Shapiro, 2021; Utset, 2021). Predictive policing is often understood as synonymous with digital cyber system-guided patrolling. Currently, academic reflection frequently links predictive policing to the "uberization" of patrolling practices (Sandhu & Fussey, 2021), which we will address later.

What we refer to as predictive police proactive actions encompass a wide spectrum of operations, not just limited to digital systems or patrolling. This operational strategy extends beyond technology use, incorporating a broad range of techniques and knowledge for predictive planning of preventive actions. Meanwhile, predictive policing often relates to the use of algorithms and digital cyber systems for directing patrols and other police operations based on extensive data analysis. Although both aim to prevent crime through prediction, predictive police proactive actions are characterized by an integrated approach, involving intense police intelligence work, whereas predictive policing focuses more on optimizing police resources through data analysis.

Throughout this theoretical study, we'll discuss the importance of police intelligence specialization, its constant evolution, and the need to adapt its doctrine to new technologies and analytical methods. Moreover, we highlight the critical need for investments in police intelligence, which involves complex and costly acquisition of equipment, systems, and human resources training. We also demonstrate how predictive police proactive actions, grounded in advanced police intelligence, can play a proactive role in preventing extreme violence, potentially transforming the public security model from reactive to proactive.

We further address significant ethical, doctrinal, and legislative challenges to conducting predictive police proactive actions in a democratic state. Legal issues like privacy preservation and technical challenges, such as the need for extensive, prolonged, and continuous professional training for police officers, are sensitive topics that must be tackled. In this context, data analysis for public security prediction presents complex legal issues, requiring a balance between violence prevention efficiency and individual rights respect.

We omit detailed discussions on the nuances of defining extreme violence, a topic demanding exclusive reflection. For our objectives, it suffices to mention activities like terrorism, crimes aimed at destabilizing democratic states (Pawelec, 2022), or school attacks orchestrated by hate groups, where prevention serves as an effective violence interruption strategy from the preparatory acts. So, predictive police proactive actions fit for certain and few threats.

In conclusion, we emphasize the critical need for substantial investments in technology, personnel training, and data infrastructure, positioning police intelligence as an essential requirement for all police operations and combating extreme violence.

SYNTHETIC CONTENT AND THE EVOLUTION OF CRIMINAL ACTIVITIES

The emergence of new threats prompts reflection on the need to bolster police intelligence, notably the production of content by digital cyber systems. In this matter, synthetic content refers to materials created or significantly altered through advanced digital technologies such as artificial intelligence and machine learning (Kalpokas, 2020). These technologies facilitate the manipulation of images, videos, and audios with an unprecedented degree of realism, which can serve either benign or nefarious purposes. Thus, the evolution of synthetic content plays a dual role in society, as atomic energy, offering innovations and presenting new challenges within the criminal activity landscape. Moreover, attention must be given to emerging issues related to cyber violence, a concept still under development (Pires, 2023b).

In this context, a pressing concern regarding synthetic content is its potential for misinformation and manipulation of the democratic process. The ability to create convincing yet false videos and audios allows malevolent actors to spread fake news or fabricate statements from public figures, unduly influencing public opinion and, by extension, the outcomes of elections and other democratic processes (Muñoz, 2024), as has occurred in recent history.

Furthermore, in the realm of child sexual abuse, synthetic content opens new avenues for the perpetuation and expansion of these crimes (Gamage et al., 2022). Sexual exploitation materials derived from real audiovisuals, often involving children and adolescents, can be manipulated or used as a basis for creating new illicit content. This not only exacerbates the trauma of the original victims but also complicates the efforts to track and suppress these crimes, as distinguishing between what is real and what is synthetic becomes increasingly challenging (Laranjeira et al., 2022).

Given this reality, it is clear that traditional police techniques and doctrines fall short in confronting advanced digital cyber systems. Effectively combating these new forms of technological crime requires substantial investment in infrastructure, training, and operational and legislative modernization. Police authorities need advanced technological resources for detection, analysis, and tracking of synthetic content, as well as legislative updates that address the specifics of this new mode of criminal organization operation. This joint effort between police force modernization and legal framework enhancement is crucial to safeguard society against the emerging risks associated with the advancement of synthetic content and cyber violence.

PREDICTIVE POLICE PROACTIVE ACTIONS WITHIN THE CONTEXT OF POLICE INTELLIGENCE

Before delving into predictive police proactive actions specifically, it is essential to clarify that police intelligence encompasses a broad spectrum of activities, acting as the backbone for the development and implementation of a wide variety of tactical and operational police operations. The intelligence products provide a robust foundation not only for predicting potential incidents but also for planning and executing various operations tailored to the specifics of each situation (Hamada & Moreira, 2022).

These operations may be carried out by intelligence units themselves or by other specialized divisions, depending on the mission's nature and the type of threat being addressed. While police intelligence work is fundamental and comprehensive, spanning from data collection, information analysis, intelligence product development, to the dissemination of operational information, predictive police proactive actions focus more narrowly on using these products to anticipate the possible occurrence of crimes and incidents with severe public order repercussions.

Hence, although prediction for police operations is valuable within the intelligence spectrum, it does not encapsulate the entire breadth of intelligence work, which is crucial for the success of any police operation. Thus, predictive police proactive actions rely intrinsically on police intelligence but are distinct, acting as a complement to its broader strategies.

Moreover, predictive police proactive actions can be framed within the context of Risk Criminal Law. Here, the crimes to which they apply are abstract danger offenses, sparking heated debate over a potential illegitimate expansion of punitive law (Carinhato, 2014;

Silveira & Fernandes, 2021). This is viewed as a violation of classical criminal law principles such as offensiveness, minimal intervention, proportionality, culpability, and legality. Ferrajoli (2002) even argues that this represents an authoritarian criminal law model. In Brazil, the expansionist approach is criticized as unconstitutional (Silveira & Fernandes, 2021), suggesting that this protection should be assigned to other branches of law, respecting the principle of minimal intervention and requiring concrete danger for penal sanction justification. In this light, this intricate debate casts predictive police proactive actions into the shadow of severe legal uncertainty, despite the social demand for crime prevention with deep repercussions on public safety. After a massacre at a school, instigated by digital hate groups, society questions whether police authorities could have done something to interrupt these criminal actions.

Equally relevant is the fact that the concept of Risk Criminal Law reflects the dynamics of globalization and contemporary technological challenges, aligning with social demands for preventive responses to new threats. This results in an increasing demand for security and more comprehensive and anticipatory state interventions. Therefore, the line between punishable and non-punishable behavior is becoming increasingly blurred, reducing the requirement for culpability and loosening criteria for attribution, a phenomenon observed worldwide.

In reflecting on predictive police proactive actions, we wish to highlight that an important aspect of this expansion is the increased risk of compromising individual freedoms, which could have hard repercussions on people's lives, including deprivation of liberty and restrictions of rights. All this must be considered in formulating police operation doctrines, control actions of police activity, and corresponding legislative development.

Considering these controversies, we suggest that predictive police proactive actions are not suitable and appropriate for every police need. However, there are specific contexts in which, exceptionally, they become important strategies for interrupting crimes with grievous outcomes. On this, Ferreira et al. (2023) argue that there has been a significant increase in school attacks in Brazil, linking them to socio-political issues and the influence of digital media in spreading hate groups. These authors reveal that the attacks, which began in the 2000s, have intensified recently, with an alarming increase in fatalities and injuries. Their analysis suggests that bullying, prolonged exposure to violent environments, and online radicalization contribute to these acts. In this context, to prevent the occurrence of mass homicides, predictive police proactive actions present themselves as a suitable and necessary measure.

This is precisely one of the objectives of this work: to highlight the suitability and challenges that predictive police proactive actions may face. In this regard, the scientific literature (Schmid, 2020; Berk, 2021; Mugari & Obioha, 2021) has indicated that the use of predictive algorithms represents a significant evolution in crime-fighting strategies, incorporating technological advancements to anticipate and prevent crimes with significant social repercussions. This approach, combining data analysis, criminological theories, predictive algorithms, and operative forces, reflects a movement towards more strategic and informed public security services, a movement explicitly observed in most democratic countries.

Regarding the history of prediction in public security actions, we identify that it began with what is known as predictive policing. On this, Duarte and Lobato (2022) tell us that its origins date back to the works of the Sociological School of Chicago in the

1920s, from their studies on recidivism. To date, the concept of predictive policing has significantly evolved from its primitive theoretical origins at the Chicago School. This school of thought emphasized the importance of social and environmental factors in understanding crime, arguing that criminal behavior was strongly influenced by the urban environment (Carneiro, 2022), which is currently considered a prejudiced premise.

The most recent version of prediction in police work (Mcdaniel & Pease, 2021) is, therefore, the result of technological evolution and advancements in data analysis, transforming the main premises of the concept. Today, this work relies heavily on the use of algorithms and the analysis of extremely large, complex, and varied data volumes, challenging conventional processing capabilities. Unlike initial approaches focused on sociological theories, the prediction for public safety uses statistical methods and machine learning to analyze large data volumes — from criminal incident records, social media content, socio-demographic information, to urban mobility patterns (Hälterlein, 2021). This technological approach allows police forces to act more effectively, enhancing crime prevention. However, this development also brings ethical concerns and issues regarding bias and privacy, challenging professionals in the field to find a balance between the efficiency of police operations and respect for individual rights.

Nonetheless, the use of artificial intelligence and other advanced strategies for collecting and analyzing digital data has proven valuable throughout the evolution of intelligence systems. However, we wish to emphasize that these technologies do not replace the indispensable human analysis, as the complexity of situations and the need for ethical and contextual judgments demand human intervention and decision-making.

It is important to highlight that the predictive police proactive actions discussed in this work are not reduced to the "uberization" of policing, a term used by Sandhu and Fussey (2021) to describe the automation of the police mission assignment process without the necessary critical reflection. Unlike the simple automatic allocation of missions, mission-oriented prediction for public safety should be understood as a support methodology that enhances, rather than replaces, the discernment and work of police intelligence analysts. This approach ensures that, while we can use artificial intelligence to identify patterns and predict potential incidents, public cooperation through reporting, police infiltration operations, critical analysis, and the final decision remain human responsibilities, aiming to ensure that technology use aligns with the ethical principles and justice of a democratic society. About this matter, Utset (2021) argues that predictive policing in public safety serves as a means to optimize the utilization of police resources in tackling crimes of significant concern.

To help in dealing with massive sets of data, algorithms play a crucial role, enabling swift and comprehensive analysis to generate accurate predictions, thereby enhancing the speed of operational decision-making processes. Artificial intelligence capabilities may soon replicate police infiltration into digital cyber systems on a much larger scale than humanly possible. In the context of potential growth among hate promotion and misinformation groups, given the scarcity of human resources, this solution should be a topic of discussion. Such a strategy might be termed the police use of social bots (Spranger et al., 2017), a complex issue that also requires in-depth debate.

In this light, predictive policing actions not only emerge as an operational tool but also as a crucial strategic component, playing a vital

role in criminal policies aimed at preventing crimes with significant social impact (Shapiro, 2021). This approach not only mirrors the ongoing adaptation of policing strategies but also gains increased importance in the face of the need to counter terrorist threats and anticipate events of extreme violence.

BEYOND ALGORITHMS: ENSURING JUSTICE IN PUBLIC SAFETY PREDICTION

Despite the significant promises and advantages predictive police proactive actions offer, it's critical to acknowledge and address their drawbacks and limitations for effective and ethical implementation. One of the foremost challenges relates to the transparency of the analytical, auditing, evaluation, and access to primary data processes (Klöckner, 2023). The algorithmic and complex nature of preliminary predictive analyses often obscures understanding of how intelligence products are generated. This lack of transparency can breed community distrust and complicate accountability for police forces. Therefore, establishing robust procedures for disclosure and explanation of these models' operations is imperative to ensure public understanding and trust in adopted practices, while still maintaining necessary operational secrecy, codes, and police techniques. Additionally, having human agents analyze the intelligence products generated by algorithms is a step that can mitigate these issues.

Another central concern is the responsibility in using predictive police proactive actions. As decisions are initially based on algorithms, there's a risk of automatically attributing a value of infallibility to certain premises, leading to possible negligence on the part of human operators. Misinterpretation or excessive confidence in predictions can result in inappropriate, unfair, or disastrous police proactive actions. Thus, it's crucial to establish clear protocols within the realm of responsibility of intelligence analysts and other security professionals, ensuring that predictive analysis supports, rather than replaces, human judgment.

Moreover, intelligence products derived from predictive techniques are susceptible to perpetuating existing biases in the data used to train algorithms. If historical data reflect inequalities or biases, predictive models can replicate and exacerbate such biases, resulting in discriminatory practices (Camillery et al., 2023). Addressing this issue requires constant review of data sets, active identification and correction of biases, and ensuring actions are aligned with ethical, equitable, and legal principles.

Therefore, the development of predictive actions demands a non-trivial and balanced approach whose intermediary products are crafted within the context of the knowledge production methodology adopted by the considered police body. This should take into account not just effectiveness in crime prevention but also transparency, responsibility, and bias mitigation to ensure this methodology yields reliable products for tackling contemporary public safety challenges.

THE NEED FOR INVESTMENT IN POLICE INTELLIGENCE

Predictive police proactive actions, driven by significant advancements in police intelligence, emerge as a potential innovative and critical response. However, this paradigm necessitates continuous investment in police intelligence, not just as an operational necessity but as a crucial strategic foundation in preventing extreme violence (Elias, 2019) associated with purely cybercrimes (Pires, 2023b) and those whose violence extends beyond the digital realm, such as election manipulation and school attacks, which can

start in virtual hate-promotion groups and end in the real environment (Neto et al., 2023).

The specialization of police forces in the context of prediction goes beyond the mere acquisition of technical knowledge or equipment. It entails a multifaceted understanding of the nuances of cybercrimes and how these illicit activities intertwine with emerging technologies, criminal organizations' purposes, and manifest in social environments. Furthermore, it involves understanding how criminals exploit individual rights and guarantees to conceal their delinquent activities. In this context, the application of artificial intelligence in developing police intelligence products represents not just an operational advantage; it's a revolution in how crime prevention and combat are conceived.

However, for this promise to be fulfilled, it's imperative to ensure transparency and guarantee audits accompany its use, protecting individual rights while seeking to improve collective security. The broad spectrum of violent cybercrimes (Pires, 2024) highlights the need for police intelligence that is not only reactive but predominantly proactive and adaptive. Predicting and preventing crimes in the virtual sphere requires an intimate and updated understanding of the methods criminals employ, as well as the technologies facilitating the planning, preparation, and execution of such crimes. Herein lies the importance of investments in specialized training and cutting-edge systems (Junior, 2023). The continuous training of police teams specialized in cybersecurity, coupled with the development and implementation of advanced technological solutions, forms the core of an effective strategy to face cybercrimes (Meijer & Wessels, 2019) and prevent extreme violence.

Moreover, the complexity and severity of cybercrimes demand a response that extends beyond the technological scope. The social ramifications of these crimes, ranging from attacks on critical infrastructure to mass homicides, underline the need for a comprehensive approach to police intelligence. This involves not only detecting and preventing criminal activities but also understanding their underlying causes and impacts. Thus, investment in police intelligence must also include sociological and psychological analysis of the perpetrators and victims of cybercrimes, as well as the development of public policies and educational initiatives aimed at reducing society's vulnerability to such threats (Pires, 2023a).

Therefore, investment in police intelligence in the era of cybercrimes represents not just a security strategy but a commitment to societal resilience. Adopting advanced analytical solutions, the continuous specialization of police forces, and a proactive and preventive approach to cybercrimes are essential to protect society in an increasingly digitized world. These investments strengthen the capacity of police forces not only to respond to current challenges but also to anticipate and adapt to future threats, thus ensuring the safety and well-being of all citizens.

LEGISLATIVE NEEDS

Implementing predictive police proactive actions in Brazil, as in any other country, entails facing various legislative challenges. These challenges are multifaceted, encompassing ethical, technical, and legal issues. For Brazilian legislators, proposing an appropriate legal framework for the use of prediction in public security operations requires careful regulation of crime prevention efficacy, protection of citizens' fundamental rights, and legal support for police work.

UPDATING LAW ON CRIMINAL ORGANIZATIONS

The complexity and constant evolution of public security threats necessitate an urgent update of sections II and III of Law 12.850, dated August 2, 2013, concerning controlled action and agent infiltration. Our argument highlights the imperative need to strengthen police intelligence practices in the face of emerging challenges, especially in the context of cybercrimes and extreme violence. The current measures do not ensure proper legal security for police officers. Integrating new practices into the existing legal system, as Moraes (2022) emphasizes the importance of a comprehensive approach in legislation on predictive police proactive actions. For instance, the potential police use of social bots, which could be classified as a form of infiltration or controlled action, represents an innovative facet in cybersecurity, particularly in combating crimes using advanced technologies, such as voter opinion manipulation through digital systems. These bots, programmed to autonomously perform specific tasks on the internet, can be employed to monitor, identify, interact with, and counter the spread of disinformation, fraudulent activities, and the formation of online manipulation networks. In this context, the police application of social bots emerges as a promising strategy, as it confronts adverse cyber systems with similar or superior capacity, offering a response commensurate with the challenges posed by modern digital criminality.

However, the use of social bots by security agencies must be accompanied by strict transparency, ethics, and human supervision protocols, ensuring their application aligns with justice principles and respect for fundamental rights. Additionally, strengthening provisions for obtaining evidence and judicial warrants based on reports from identified individuals is necessary, ensuring the absolute confidentiality of their accounts or cooperation with intelligence operations. In the current legal context, reporting is the most practical tool for demonstrating the potential preparation of a criminal activity and justifying judicial or police intervention, such as infiltration actions or privacy restrictions for conducting investigations in the digital context.

WAR GAMES: MODELING LEGAL DYNAMICS IN THE FIGHT AGAINST CRIMINAL ORGANIZATIONS

One effective approach to address the intricate task of identifying legislative needs for updating laws concerning criminal organizations is the implementation of war game simulations. In these simulations, participants assume three distinct roles: (1) criminals, who operate with minimal constraints, embodying the unbridled nature of organized crime; (2) legal forces, tasked with countering the simulated criminal activities within the constraints of current legislation; and (3) a group that engages in combating the criminal simulations within a dynamic legal framework, which evolves based on general principles but aims to keep pace with the fluid dynamics of criminal organizations. This method allows for a comprehensive evaluation of existing legal structures and their efficacy in real-world scenarios. By observing the interactions and outcomes of these simulations, lawmakers and policy developers can gain valuable insights into the gaps and inefficiencies in current laws. The dynamic legal framework group, in particular, provides a testing ground for adaptive legislative changes, offering a pragmatic preview of how new or revised laws might perform against the evolving tactics of organized crime, thereby informing more targeted and effective legislative updates.

DATA PROTECTION AND PUBLIC SECURITY: ADDRESSING EXTREME VIOLENCE IN THE CONTEXT OF LGPD

Balancing security and privacy illustrates the complexity of employing predictive technologies in public security contexts. As Strikwerda (2021) and Alikhademi et al. (2022) argue, the main task lies in reconciling imperative public security with safeguarding fundamental rights to privacy and data protection, a challenge amplified by the Brazilian General Data Protection Law (LGPD). This legislation, while significant, requires refinements to address security practices' specificities, ensuring appropriate data treatment and implementing robust oversight mechanisms that protect privacy (Pires, 2024).

In this matter, the necessity of valorizing witness reports as a cornerstone for predictive policing, and the imperative of enhancing witness protection laws, are grounded in several compelling reasons. Firstly, informant tips provide critical preemptive insights that enable law enforcement to disrupt criminal activities before they escalate, thus playing a pivotal role in predictive policing strategies. These reports serve as proactive tools, offering real-time data that can be analyzed to foresee and mitigate potential threats.

Secondly, the effectiveness of such predictive measures is closely tied to the protection and confidence of those who provide these crucial insights. Enhanced witness protection laws are essential to safeguard these informants from potential reprisals, thereby ensuring a steady flow of valuable information. Strengthening these protections not only bolsters the credibility and viability of law enforcement interventions but also encourages more citizens to come forward with vital information.

TRANSPARENCY AND ACCOUNTABILITY IN PUBLIC SECURITY

Transparency and accountability in data collection and analysis are fundamental to sustaining public trust in security operations. As Bakke (2018) discusses, establishing a regulatory framework that allows inter-institutional supervision over the use of data and predictive analysis algorithms, introducing accountability mechanisms to prevent abuses and errors, is crucial. This framework must align with the principles of legality, impersonality, morality, publicity, and efficiency governing public administration. The lack of transparency and access to information about data collection and use in public security highlights the need to strengthen access to information laws, ensuring transparency in these activities and building trust between citizens and security authorities.

ADDRESSING ALGORITHMIC BIAS IN LAW ENFORCEMENT

Furthermore, preventing algorithmic bias is a central concern, pointed out by Van Brakel (2021), who suggests implementing regular and independent audits of artificial intelligence systems to avoid discrimination, thus promoting the delivery of assertive and equitable intelligence products and mitigating the ever-present possibility of bias in law enforcement.

UPDATING LAW TO ENSURE PROTECTION AGAINST AUTHORITY ABUSE

Protecting against authority abuse is also essential to ensure that police proactive actions operate within an appropriate and legal justification framework. As Yen and Hung (2021) discuss, establishing clear limits for the use of surveillance technologies, including

the need for judicial authorizations, is vital to protect citizens against mass surveillance and ensure fundamental rights. Additionally, specific sanctions should be envisaged for the misuse of digital cyber systems in the context of authority abuse (Law 13.869, dated September 5, 2019).

TRAINING AND ETHICS: PILLARS FOR POLICE EFFICIENCY IN THE ERA OF PREDICTIVE TECHNOLOGIES

Continued education, enhancement, and police training are critical elements for the effective implementation of predictive technologies. Investments in ongoing training and resources enabling public security professionals to operate, develop, and refine this approach within an ethical, legal, and operational framework are indispensable.

SCIENTIFIC AND OPERATIONAL INTELLECTUAL PRODUCTION PROMOTED BY CENTRAL PUBLIC SECURITY AGENCIES

Knowledge production plays a crucial role in advancing predictive police proactive actions, providing the necessary scientific and technical basis for developing more efficient and effective strategies to confront criminality. Incorporating updated police doctrine, the most advanced techniques, and especially the latest technological aspects, is essential to keep security forces ahead of the tactics employed by constantly evolving criminals.

In this context, central public security agencies should promote a robust scientific and technological development plan that not only fosters applied research in critical areas for public security but also ensures ongoing training and specialization of professionals in the field. This strategic approach allows not only adaptation to emerging threats but also anticipation of new challenges, ensuring a proactive and evidence-based response to society's security needs.

To ensure the integrity and impact of this research effort, establishing an academic validation system that maintains necessary secrecy while recognizing and valuing researchers' contributions within their academic and professional trajectory is imperative. A viable proposal would be the use of existing and protected systems, like the Unified Public Security System, adapted to allow peer review and dissemination of studies and innovations only to individuals with appropriate security credentials. This mechanism not only preserves the security of sensitive information but also promotes an environment of incentive for innovation and academic recognition within public security institutions. Through this research support structure, a culture of continuous improvement and operational excellence can be cultivated, essential for addressing the complex challenges of contemporary security.

STRENGTHENING THE PARTNERSHIP BETWEEN SCIENTIFIC PRODUCTION AND THE PUBLIC SECURITY PRODUCT INDUSTRY

Promoting the development of a national industry for public security products, especially digital cyber systems, is a pressing need in the current context, where predictive police proactive actions are increasingly important in combating criminality. The ability to anticipate criminal acts, especially those using the vast digital arena to perpetrate crimes like election manipulation or coordination of terrorist attacks, crucially depends on technological advancement and the implementation of innovative solutions. Collaboration between security forces and the industrial sector, supported by a robust science, technology, and research segment, is vital to

translate academic and technical knowledge into products that can be employed in the operational context. This joint effort should aim to create an ecosystem that not only develops but also continuously implements and enhances the necessary technologies to keep society safe against emerging threats.

Implementing public policies that encourage partnerships between the security sector, industry, and academic institutions is crucial to ensure that advancements in the security field are not just conceptual but materialize into tangible and effective solutions. The synergy between these sectors can accelerate the development of predictive technologies, advanced surveillance systems, and other vital tools for effectively combating organized crime and other forms of extreme violence.

THE IMPERATIVE NEED FOR INTERNATIONAL AND INTER-INSTITUTIONAL COOPERATION IN DIGITAL CYBERSECURITY

International cooperation plays a crucial role in addressing transnational security challenges, especially cyber ones. Collaboration among nations, in harmony with international data protection and human rights agreements, is essential for an effective and respectful response to global threats, highlighting the importance of multilateral strategies in legislation and security practices. Besides, inter-agency cooperation must be enhanced, even the organizational law of the intelligence system should be reviewed.

CONCLUSION

In this study, we emphasize the critical importance of strengthening police intelligence in combating extreme violence, highlighting the need for substantial investments in technology, personnel training, and data infrastructure. We argue that a predictive approach, grounded in advanced intelligence, is essential for effectively preventing such acts of violence, promoting a shift from a reactive to a proactive public security model, despite the profound paradoxes awaiting resolution.

The use of surveillance technologies brings the dilemma of their potential for overuse, impacting individual freedom. Developing legislation to regulate this use, establishing criteria for necessity, proportionality, and transparency, is necessary to ensure that surveillance technologies serve the public interest without violating individual rights.

The effectiveness and ethics of applying predictive technologies require a regulatory framework that sets standards, ensuring these technologies are used fairly and efficiently in public security. Social control over public security measures and the use of technologies underlines the importance of encouraging citizen participation and external oversight of these policies, ensuring citizens' voices are considered.

Implementing predictive police proactive actions demands ongoing dialogue among legislators, security experts, technology professionals, legal experts, and civil society to develop a legislative framework that protects citizens from both crime and potential excesses in surveillance and personal data use. This balanced approach must respect the principles of legality, morality, publicity, and efficiency, ensuring transparency, accountability, and the prevention of algorithmic bias in public security practices.

Proposing a legislative framework for predictive police proactive actions in Brazil is, therefore, a complex process that requires a balanced approach, protecting citizens from both crime and potential excesses in surveillance and personal data use. The key to success lies in ongoing dialogue among legislators, security experts, technology professionals, legal experts, and society.

International Journal of Human Sciences Research ISSN 2764-0558 DOI: https://doi.org/10.22533/at.ed.5584162408054

We conclude that police intelligence, supported by adequate investments and a robust legislative framework, represents a fundamental pillar in combating extreme violence. Predictive police proactive actions, when applied ethically and effectively, have the potential to transform public security, making it more proactive, fair, and aligned with fundamental rights, thus establishing a safer and more resilient social environment.

REFERENCES

Alikhademi, K., et al. (2022). A review of predictive policing from the perspective of fairness. *Artificial Intelligence and Law, 1-17*. https://doi.org/10.1007/s10506-021-09286-4

Bakke, E. (2018). Predictive policing: the argument for public transparency. *NYU Annual Survey of American Law, 74*, 131.

Berk, R. A. (2021). Artificial intelligence, predictive policing, and risk assessment for law enforcement. *Annual Review of Criminology, 4*, 209-237. https://doi.org/10.1146/annurev-criminol-051520-012342

Camilleri, H., et al. (2023). Media coverage of predictive policing: Bias, police engagement, and the future of transparency. In *Proceedings of the 3rd ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization* (pp. 1-19). https://doi.org/10.1145/3617694.3623249

Carinhato, P. H., et al. (2014). Os crimes de perigo abstrato e a expansão do direito penal. *Argumenta Journal Law, 20*, 63-80.

Carneiro, L. de A. (2022). Uma revisão sobre a Teoria da Desorganização Social. *Revista do Instituto Brasileiro de Segurança Pública, 5*(13), 9-30.

Duarte, D. E., & Lobato, L. C. (2021). A política do policiamento preditivo: pressupostos criminológicos, técnicas algorítmicas e estratégias punitivas. *Revista Brasileira de Ciências Criminais*, 57-98.

Elias, L. (2019). O terrorismo transnacional contemporâneo: Segurança, justiça e cooperação. *Nação e Defesa, 152*, 78-112.

Ferrajoli, L. (2002). *Direito e Razão: Teoria do Garantismo Penal*. São Paulo: Revista dos Tribunais.

Ferreira, V. de J., Santos, M. S. dos, & Oriente, S. B. (2023). O cenário da violência em destaque: discutindo os atuais ataques nas escolas de educação básica no Brasil. *Revista Transmutare, 8*.

Gamage, D., et al. (2022). Are deepfakes concerning? analyzing conversations of deepfakes on reddit and exploring societal implications. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (pp. 1-19).

Hälterlein, J. (2021). Epistemologies of predictive policing: Mathematical social science, social physics and machine learning. *Big Data & Society, 8*(1), 20539517211003118. https://doi.org/10.1177/20539517211003118

Hamada, H. H., & Moreira, R. P. (2020). A inteligência estratégica como atividade essencial para as instituições de segurança pública. *Cadernos de Segurança Pública, 12*, 4-16.

Junior, A. de O. (2023). Posfácio – A Importância das Atividades de Investigação e Inteligência Policial para o Sistema de Justiça Criminal e seu Aperfeiçoamento no Brasil. *Boletim de Análise Político-Institucional*. https://doi.org/10.38116/bapi33art10

Kalpokas, I. (2020). Problematising reality: the promises and perils of synthetic media. *SN Social Sciences, 1*(1), 1-11. https://doi.org/10.1007/s43545-020-00010-8

Klöckner, C. (2023). *A capacidade de controle externo das atividades de inteligência na era digital* [Doctoral dissertation, Fundação Getúlio Vargas, Rio de Janeiro].

Laranjeira da Silva, C., Macedo, J., Avila, S., & Santos, J. (2022). Seeing without looking: Analysis pipeline for child sexual abuse datasets. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (pp. 2189-2205).

McDaniel, J., & Pease, K. (Eds.). (2021). *Predictive policing and artificial intelligence*. Routledge. https://doi.org/10.4324/9780429265365

Meijer, A., & Wessels, M. (2019). Predictive policing: Review of benefits and drawbacks. *International Journal of Public Administration, 42*(12), 1031-1039. https://doi.org/10.1080/01900692.2019.1575664

Moraes, F. (2022). *Policiamento Preditivo e aspectos constitucionais*. Editora Dialética. https://doi.org/10.48021/978-65-252-5566-8

Mugari, I., & Obioha, E. E. (2021). Predictive policing and crime control in the United States of America and Europe: trends in a decade of research and the future of predictive policing. *Social Sciences, 10*(6), 234. https://doi.org/10.3390/socsci10060234

Muñoz, K. (2024). The AI Election Year: How to Counter the Impact of Artificial Intelligence. *DGAP-Memo*. https://nbn-resolving.org/urn:nbn:de:0168ssoar-92636-3

Neto, J. L. T., et al. (2023). Perfil criminológico de agressores em ataques a escolas: características, motivações e prevenção. In *Educação em foco: tópicos relevantes e pesquisas recentes* (pp. 43-56), RFB.

Pawelec, M. (2022). Deepfakes and democracy (theory): How synthetic audio-visual media for disinformation and hate speech threaten core democratic functions. *Digital Society, 1*(2), 1-37. https://doi.org/10.1007/s44206-022-00010-6

Pires, S. F. S. (2024). Desafios da interação online: enfrentando a violência extrema para garantir direitos fundamentais. In A. W. S. de Vasconcelos (Ed.), *Caminhos da justiça: explorando o mundo do direito 2* (pp. 36-51). São Paulo: Atena. https://doi.org/10.22533/at.ed.0852409013

Pires, S. F. S. (2023). Enfrentamento sustentável e integral à violência e aos preconceitos na escola: um desafio complexo, mas viável. *Contemporânea, 3*, 8012-8038. https://doi.org/10.56083/rcv3n7-036

Pires, S. F. S. (2023). Violência cibernética: a inteligência artificial é autônoma? *Cadernos Aslegis, 62*, 163-174.

Sandhu, A., & Fussey, P. (2021). The 'uberization of policing'? How police negotiate and operationalise predictive policing technology. *Policing and Society, 31*(1), 66-81. https://doi.org/10.1080/10439463.2020.1803315

Schmid, A. P. (Ed.). (2020). *Handbook of terrorism prevention and preparedness*. International Centre for Counter-Terrorism (ICCT).

Shapiro, A. (2021). Accountability and indeterminacy in predictive policing. In *Predictive Policing and Artificial Intelligence* (pp. 185-213). Routledge. https://doi.org/10.4324/9780429265365-10

Silveira, D. R., & Fernandes, F. A. (2021). Acerca dos crimes de perigo abstrato-concreto na doutrina geral dos crimes de perigo. *IUS ET VERITAS: Revista de la Asociación IUS ET VERITAS, 62*, 204-214.

Spranger, M., et al. (2017). The infiltration game: Artificial immune system for the exploitation of crime relevant information in social networks. In *Proceedings of the Seventh International Conference on Advances in Information Management and Mining (IMMM)*, ThinkMind Library (pp. 24-27).

Strikwerda, L. (2021). Predictive policing: The risks associated with risk assessment. *The Police Journal, 94*(3), 422-436. https://doi.org/10.1177/0032258x20947749

Utset, M. A. (2021). Predictive policing and criminal law. In *Predictive Policing and Artificial Intelligence* (pp. 163-182). Routledge. https://doi.org/10.4324/9780429265365-8

Van Brakel, R. (2020). Rethinking predictive policing. In *The Algorithmic Society: Technology, Power, and Knowledge* (p. 43). https://doi.org/10.4324/9780429261404-9

Yen, C.-P., & Hung, T.-W. (2021). Achieving equity with predictive policing algorithms: a social safety net perspective. *Science and Engineering Ethics, 27*, 1-16. https://doi.org/10.1007/s11948-021-00312-x