DIGITAL SECURITY TECHNOLOGIES AND THE RECONFIGURATION OF THE CRIME TRIANGLE: EVIDENCE OF THE STRENGTHENING OF THE "CAPABLE GUARDIAN" IN THE CONTEXT OF THE STATE OF TOCANTINS

TECNOLOGIAS DE SEGURANÇA DIGITAL E A RECONFIGURAÇÃO DO TRIÂNGULO DO CRIME: EVIDÊNCIAS DO FORTALECIMENTO DO "GUARDIÃO CAPAZ" NO CONTEXTO DO ESTADO DO TOCANTINS

TECNOLOGÍAS DE SEGURIDAD DIGITAL Y LA RECONFIGURACIÓN DEL TRIÁNGULO DEL DELITO: EVIDENCIAS DEL FORTALECIMIENTO DEL "GUARDIÁN CAPAZ" EN EL CONTEXTO DEL ESTADO DE TOCANTINS

https://doi.org/10.56238/sevened2026.024-002

Marcos Antonio Negreiros Dias[1], Dernivaldo da Costa Tirello[2], Rachel Barbosa Lopes Cavalcante Tirello[3], Daniel Silva dos Santos[4], José Elianeo de Souza Pereira[5], Benício da Costa Neves[6], Marcel Sales Campelo[7], Sérgio Vieira da Silva[8]

ABSTRACT

The increasing complexity of contemporary crime has driven the incorporation of digital technologies as a central strategy in public security, especially in the context of smart cities. In this scenario, the problem arises of understanding how these technologies contribute to the reconfiguration of the conditions that favor the occurrence of crime, in light of the Crime Triangle Theory. Thus, the present study aimed to analyze how security technologies, especially video surveillance systems and digital applications, act in the reconfiguration of the elements of the Crime Triangle in the State of Tocantins. Methodologically, this is a qualitative, descriptive, and exploratory literature review, conducted based on the PRISMA protocol and Bardin's content analysis. Data collection was carried out in the Scopus, Web of Science, and Google Scholar databases, resulting in a final corpus of 20 analyzed studies. The results show that security technologies predominantly act in strengthening the "capable guardian" through the expansion of surveillance, response capacity, and data integration. It

[1] Doctoral Student in Forest and Environmental Sciences. Universidade Federal do Tocantins (UFT). E-mail: marconegreiros1985@gmail.com Orcid: https://orcid.org/0000-0003-1964-620X
[2] Master's Student in Fundamental Rights and Alterity. Universidade Católica de Salvador (UCSAL). E-mail: tirelopm@gmail.com Orcid: https://orcid.org/0009-0002-5842-4319
[3] Doctoral Student in Constitutional Law. Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP). E-mail: rachelblc@hotmail.com Orcid: https://orcid.org/0009-0001-6182-7947
[4] Master's Student in Public Policy Management. Universidade Federal do Tocantins (UFT). E-mail: daniel.santos2@mail.uft.edu.br Orcid: https://orcid.org/0009-0007-5137-6955
[5] Specialist in Strategic Planning and Management in Public Security. Universidade Estadual do Tocantins (UNITINS). E-mail: elibanderas@gmail.com Orcid: https://orcid.org/0009-0003-4767-861X
[6] Master's degree in Police Sciences. Academia Policial Militar Tiradentes (APMT). E-mail: nevesbenicio@gmail.com Orcid: https://orcid.org/0009-0005-9802-7184
[7] Doctoral Student in Police Sciences of Security and Public Order. Centro de Autos Estudos em Segurança (CAES). E-mail: marcelsalescampelo@gmail.com Orcid: https://orcid.org/0009-0001-4122-4815
[8] MBA in Leadership, Management and Advisory in Public Security. Academia Policial Militar Tiradentes (APMT). E-mail: sergiovieirasi@gmail.com

was also observed that collaborative applications contribute to reducing the vulnerability of the “suitable target,” while systems based on artificial intelligence and data analysis increase the perceived risk for the “motivated offender,” albeit indirectly. However, the effectiveness of these technologies depends on factors such as institutional integration, infrastructure, and professional training. It is concluded that security technologies reconfigure the elements of the Crime Triangle, with greater impact on strengthening the guardian, constituting relevant tools for crime prevention, provided they are integrated into institutional strategies and adapted to the local context.

Keywords: Situational Crime Prevention. Digital Surveillance. Predictive Analysis. Smart Public Security.

RESUMO

A crescente complexidade da criminalidade contemporânea tem impulsionado a incorporação de tecnologias digitais como estratégia central na segurança pública, especialmente no contexto das cidades inteligentes. Nesse cenário, emerge o problema de compreender como essas tecnologias contribuem para a reconfiguração das condições que favorecem a ocorrência do crime, à luz da Teoria do Triângulo do Crime. Assim, o presente estudo teve como objetivo analisar de que forma as tecnologias de segurança, especialmente sistemas de videomonitoramento e aplicativos digitais, atuam na reconfiguração dos elementos do Triângulo do Crime no Estado do Tocantins. Metodologicamente, trata-se de uma revisão de literatura de abordagem qualitativa, descritiva e exploratória, conduzida com base no protocolo PRISMA e na análise de conteúdo de Bardin. A coleta de dados foi realizada nas bases Scopus, Web of Science e Google Acadêmico, resultando em um corpus final de 20 estudos analisados. Os resultados evidenciam que as tecnologias de segurança atuam predominantemente no fortalecimento do “guardião capaz”, por meio da ampliação da vigilância, da capacidade de resposta e da integração de dados. Observou-se também que aplicativos colaborativos contribuem para a redução da vulnerabilidade do “alvo adequado”, enquanto sistemas baseados em inteligência artificial e análise de dados aumentam o risco percebido pelo “infrator motivado”, embora de forma indireta. Contudo, a efetividade dessas tecnologias depende de fatores como integração institucional, infraestrutura e capacitação profissional. Conclui-se que as tecnologias de segurança reconfiguram os elementos do Triângulo do Crime, com maior impacto no fortalecimento do guardião, constituindo instrumentos relevantes para a prevenção criminal, desde que integradas a estratégias institucionais e adaptadas ao contexto local.

Palavras-chave: Prevenção Situacional do Crime. Vigilância Digital. Análise Preditiva. Segurança Pública Inteligente.

RESUMEN

La creciente complejidad de la criminalidad contemporánea ha impulsado la incorporación de tecnologías digitales como estrategia central en la seguridad pública, especialmente en el contexto de las ciudades inteligentes. En este escenario, surge el problema de comprender cómo estas tecnologías contribuyen a la reconfiguración de las condiciones que favorecen la ocurrencia del delito, a la luz de la Teoría del Triángulo del Delito. Así, el presente estudio tuvo como objetivo analizar de qué forma las tecnologías de seguridad, especialmente los sistemas de videovigilancia y las aplicaciones digitales, actúan en la reconfiguración de los elementos del Triángulo del Delito en el Estado de Tocantins. Metodológicamente, se trata de una revisión de literatura de enfoque cualitativo, descriptivo y exploratorio, realizada con base en el protocolo PRISMA y el análisis de contenido de Bardin. La recolección de datos se llevó a cabo en las bases Scopus, Web of Science y Google Académico, resultando en un corpus final de 20 estudios analizados. Los resultados evidencian que las tecnologías de

seguridad actúan predominantemente en el fortalecimiento del “guardián capaz”, mediante la ampliación de la vigilancia, la capacidad de respuesta y la integración de datos. También se observó que las aplicaciones colaborativas contribuyen a reducir la vulnerabilidad del “objetivo adecuado”, mientras que los sistemas basados en inteligencia artificial y análisis de datos aumentan el riesgo percibido por el “delincuente motivado”, aunque de forma indirecta. Sin embargo, la efectividad de estas tecnologías depende de factores como la integración institucional, la infraestructura y la capacitación profesional. Se concluye que las tecnologías de seguridad reconfiguran los elementos del Triángulo del Delito, con mayor impacto en el fortalecimiento del guardián, constituyendo instrumentos relevantes para la prevención del delito, siempre que estén integradas en estrategias institucionales y adaptadas al contexto local.

Palabras clave: Prevención Situacional del Delito. Vigilancia Digital. Análisis Predictivo. Seguridad Pública Inteligente.

1 INTRODUCTION

Contemporary public security has been deeply impacted by the growing complexity of criminal phenomena, driven by social, urban, and technological transformations that challenge traditional models of prevention and control. In this scenario, a paradigmatic transition from predominantly reactive approaches to data- and technology-driven preventive strategies is observed, especially in the context of smart cities. The incorporation of digital systems, such as video surveillance, artificial intelligence, data mining, and security applications, has expanded the capacity of police institutions to monitor, analyze, and respond to criminal dynamics in a more efficient and integrated manner (Hamada; Nassif, 2018; Ishaphiad; Bagula, 2020; Laufs; Borrion; Bradford, 2020).

In the field of criminology, the understanding of the occurrence of crime has been strongly influenced by the Theory of Routine Activities, which underlies the Crime Triangle, according to which criminal practice results from the convergence between motivated offender, appropriate target (victim) and absence of a capable guardian/crime scene. This perspective has guided situational prevention strategies, in which the modification of environmental conditions and the strengthening of surveillance act directly to reduce criminal opportunities. In this sense, security technologies emerge as central tools in the reorganization of these elements, by expanding surveillance, reducing the vulnerability of victims, and increasing the risk perceived by offenders (Moyo, 2019; Suslov, 2025; Abdullahi et al., 2025).

Several studies show the potential of digital technologies in crime prevention, highlighting the role of video surveillance (CCTV) in deterring crimes and producing evidence (Papale, 2023; Abdullahi et al., 2025), as well as the use of data-driven intelligent systems to identify criminal patterns and support decision-making in urban control centers (Leal & Gomes-jr., 2022; Choi; Na & Lee, 2024). In addition, collaborative applications and digital platforms have expanded social participation in public security, contributing to the construction of distributed surveillance networks and strengthening informal control (Kadar et al., 2016; Ogbu; Excellence, 2025). At the same time, data-driven policing has been consolidated as a relevant strategy, by integrating real-time information and statistical analysis into police action, promoting greater efficiency and predictive capacity (Drenth; Van Steden, 2020).

However, despite the technological advances and empirical evidence available, the literature points out that the effectiveness of these tools in crime prevention is not homogeneous, being conditioned to factors such as infrastructure, institutional integration, data governance, and training of professionals. Studies indicate that the simple adoption of

technologies does not guarantee the reduction of crime, and there may be operational limitations, displacement of crime, and challenges related to privacy and social control (Mihale-Wilson; Felka; Hinz, 2019; Laufs, 2022). In addition, the implementation of these technologies in specific institutional contexts, such as police organizations, requires structural and operational adaptations that are still in the process of consolidation (Miranda et al., 2020).

In the Brazilian context, the challenges of public security are even more complex, marked by regional inequalities and heterogeneous criminal dynamics. Data from the Brazilian Forum on Public Security indicate the persistence of high crime rates, especially in property crimes and urban violence, reinforcing the need for innovative and evidence-based strategies (FBSP, 2025). In this scenario, initiatives such as the use of institutional applications and digital systems by the military police represent important advances in the modernization of management and in the improvement of operational efficiency, as evidenced in the case of the PMTO Mobile system, which has contributed to the improvement of police service and the integration of information in the State of Tocantins (Ferreira et al., 2022; Tavares; Fernandes; Oliveira, 2023).

Despite this set of evidence, there is a significant gap in the literature regarding the integrated analysis between security technologies, Crime Triangle Theory and specific regional contexts, especially in the State of Tocantins. Although there are studies on smart cities and surveillance technologies, few studies systematically address how these tools act to break the elements of crime in local realities marked by structural inequalities and institutional limitations (Laufs; Borrion; Bradford, 2020; Laufs, 2022).

In view of this scenario, the following research problem emerges: how have security technologies, especially video surveillance systems and digital applications, contributed to the rupture of the elements of the Crime Triangle Theory in the State of Tocantins?

In view of this scenario, the present investigation is justified by the need to understand, in an integrated way, the role of security technologies in crime prevention, especially in regional contexts still little explored by the literature, such as the State of Tocantins. The analysis of these tools in the light of the Crime Triangle Theory allows us to advance in the understanding of how technology can act in breaking the conditions that favor the criminal occurrence, contributing both to the theoretical development and to the improvement of public security policies.

Thus, this article aimed to analyze the effectiveness of security technologies in crime prevention, in the light of the Crime Triangle Theory, focusing on the context of the State of Tocantins, seeking to understand how these tools act in the reorganization of the conditions that favor the occurrence of crime.

2 METHODOLOGY

The present study is characterized as a qualitative, descriptive and exploratory literature review, structured based on the guidelines of the PRISMA protocol (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*) and on the content analysis technique proposed by Laurence Bardin, with the objective of ensuring methodological rigor, transparency and reproducibility in the selection process. organization and interpretation of data. The methodological approach adopted allowed a critical analysis of the scientific production related to the use of security technologies in crime prevention, in the light of the Crime Triangle Theory, focusing on the context of smart cities and their application in the State of Tocantins.

Data collection was carried out through systematized searches in three databases widely recognized in the academic environment: *Scopus, Web of Science (*WoS) and Google Scholar. The choice of these databases is justified by their interdisciplinary scope and relevance in the indexing of studies in the areas of public security, criminology, digital technologies and smart urbanism. Structured search strategies with Boolean operators were used, combining descriptors related to four main axes: crime prevention, *Routine Activity Theory*, smart cities and security technologies, including terms such as *"crime prevention", "crime triangle", "routine activity theory", "smart city", "CCTV", "digital surveillance" and "security technology*". The time frame adopted comprised the period from 2000 to 2026, considering the consolidation and expansion of digital technologies applied to public security in this interval.

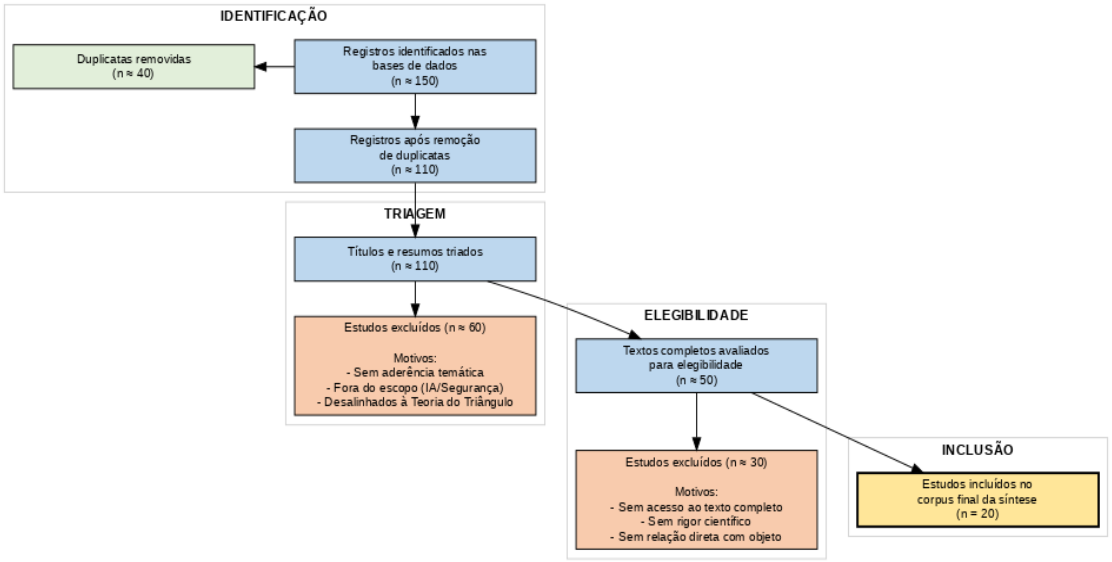
The study selection process strictly followed the steps of the PRISMA protocol. In the identification phase, approximately 150 records were recovered in the consulted databases. After consolidating the data in a single database, duplicates were removed, resulting in about 110 unique studies. In the screening stage, the titles and abstracts were read, and approximately 60 studies were excluded because they did not present thematic adherence to the scope of the research, especially those that did not directly address the relationship between technology and crime prevention or that did not align with the perspective of the Crime Triangle Theory. Thus, about 50 potentially relevant studies remained.

In the eligibility phase, the selected texts were read in full, with strict application of the previously defined inclusion and exclusion criteria. Studies that addressed technologies applied to public security, situational crime prevention, smart cities or digital surveillance, published in Portuguese or English, and that presented consistent theoretical or empirical foundations were included. Duplicate works, studies without access to the full text, productions without scientific rigor, and those that did not establish a direct relationship with

the object of study were excluded. As a result, approximately 30 studies were excluded at this stage, leaving a final corpus composed of 20 studies, as shown in Figure 1.

Figure 1

Research Selection Flowchart



Source: The authors (2026).

Data analysis was conducted using Laurence Bardin's content analysis technique, structured in three main phases: pre-analysis, exploration of the material and treatment of the results. In the pre-analysis phase, the corpus was organized, the texts were read fluctuatingly, and the analytical categories were defined, guided by the elements of the Crime Triangle (motivated offender, appropriate target, and capable guardian) and by the technological dimensions associated with crime prevention. In the material exploration stage, the contents were codified, patterns were identified, and the studies were classified according to the established categories, allowing the analysis of how different technologies impact each element of the triangle. Finally, in the treatment and interpretation phase, the data were synthesized and interpreted in the light of the adopted theoretical framework, enabling the identification of convergences, divergences and gaps in the literature.

To systematize the results, an analysis matrix was elaborated containing information on perpetrators, technologies used, elements of the Crime Triangle affected, and main contributions of the studies, as shown in Table 1. This strategy allowed a comparative and integrated analysis of the evidence, contributing to the construction of a critical and reasoned interpretation. The reliability of the research was ensured through the rigorous application of the PRISMA protocol, the clear definition of the selection criteria and the triangulation of sources and methods, ensuring consistency and validity to the results obtained.

Table 1

Content Analysis Matrix (Bardin)

Author	Technology/Approach	Analytical Category	Crime Triangle	Unit of Analysis	Interpretative Synthesis
Abdullahi et al. (2025)	CCTV	Electronic surveillance	Capable Guardian	Urban monitoring	Reduces crime by increasing surveillance and perceived risk
Choi et al. (2024)	Intelligent Systems (CPTED + AI)	Situational Avoidance	Capable Guardian	Decision making	Intelligent technologies optimize preventive decisions
Drenth; Van Steden (2020)	Data-driven policing	Police management	Capable Guardian	Police interaction	Data increases efficiency and strategic action
Ferreira et al. (2022)	PMTO Mobile	Operational technology	Capable Guardian	Police service	Agility and integration improve crime response
FBSP (2025)	Crime data	Empirical context	All	Crime indicators	Highlights the need for technological strategies
Hamada; NasSIF (2018)	Smart cities	Urban security	Capable Guardian	Urban infrastructure	Technology integrates security and urban management
Ishaphiad; Bagula (2020)	Big Data/Data Mining	Criminal intelligence	Motivated offender	Criminal patterns	Allows anticipation of criminal behavior
Kadar et al. (2016)	Collaborative apps	Social surveillance	Suitable target	Data sharing	Reduces vulnerability through social cooperation
Laufs (2022)	Technologies in smart cities	Critical analysis	All	Digital infrastructure	Effectiveness depends on integration and governance
Laufs; Borrion; Bradford (2020)	Smart cities	Systematic review	All	Urban systems	Technology expands prevention, but with limitations
Leal; Gomes-Jr. (2022)	Smart monitoring	Urban intelligence	Motivated offender	Spatial patterns	Detects changes in crime
Mihale-WiLSON et al. (2019)	Smart lighting	Environmental prevention	Suitable target	Urban environment	Reduces criminal opportunities
Miranda et al. (2020)	Institutional digital system	Public management	Capable Guardian	Administrative proceedings	Increases efficiency and transparency

Author	Technology/Approach	Analytical Category	Crime Triangle	Unit of Analysis	Interpretative Synthesis
Moyo (2019)	CCTV	Urban surveillance	Capable Guardian	Case Studies	Effectiveness depends on implementation
Ogbu; Excellence (2025)	ICT security	Educational technology	Capable Guardian	Institutional environment	Technology improves security in institutions
Papale (2023)	CCTV Operators	Operational surveillance	Capable Guardian	Human monitoring	Efficiency depends on human action
Suslov (2025)	Crime prevention	Theoretical basis	All	Criminological theory	Underpins situational prevention
Tavares et al. (2023)	PMTO Mobile	Applied technology	Capable Guardian	Operationalization	Benefits and limitations of police technology

Source: The authors (2026).

In this way, the methodology adopted enabled a comprehensive and in-depth analysis of the literature, allowing us to understand how security technologies act in crime prevention, especially in the context of smart cities, and how these mechanisms can be interpreted in the light of the Crime Triangle Theory, with direct implications for the reality of public security in the State of Tocantins.

3 LITERATURE REVIEW

3.1 PUBLIC SAFETY AND TECHNOLOGICAL INNOVATION

Contemporary public security has undergone a process of paradigmatic transformation, characterized by the transition from reactive models to preventive approaches guided by data and technology. In this context, the incorporation of digital tools and intelligent systems has been consolidated as a central element in the modernization of police institutions, allowing greater efficiency in crime management and strategic decision-making. This movement is directly associated with the advancement of the so-called smart cities, in which the integration of technology, governance, and urban infrastructure contributes to the improvement of public services, including security (Hamada; Nassif, 2018).

Technological innovation in public security involves the use of devices and systems capable of collecting, processing, and analyzing large volumes of data, enabling real-time monitoring and the identification of criminal patterns. Technologies such as video surveillance (CCTV), predictive analytics systems, artificial intelligence, and mobile security applications

have expanded the surveillance and response capabilities of security forces, making policing more proactive and evidence-driven. Studies show that these tools allow not only the detection of occurrences, but also the anticipation of criminal behaviors, contributing to the reduction of criminal opportunities (Isafiade; Bagula, 2020).

In addition, the use of digital technologies has favored the development of data-driven *policing*, in which operational decisions are based on statistical analysis and patterns identified in criminal databases. This model represents a significant advance in relation to traditional practices, by allowing a more precise and efficient performance of police teams, especially in complex urban contexts. In this sense, the interaction between technology and police practice redefines the role of the security agent, who also starts to act as an information analyst and risk manager (Drenth; Van Steden, 2020).

In the field of smart cities, the application of technologies aimed at public safety has expanded through integrated systems that combine urban sensors, digital platforms, and data visualization tools. These solutions allow for the continuous monitoring of occurrences and the identification of changes in crime patterns, subsidizing more assertive preventive actions. Tools based on data mining and spatio-temporal analysis have shown great potential in identifying criminal trends, contributing to the formulation of more effective control and prevention strategies (Isafiade; Bagula, 2020; Leal; Gomes-Jr., 2022).

However, despite the advances provided by technological innovation, its implementation in public security still faces significant challenges, especially in relation to infrastructure, systems integration, and training of professionals. The adoption of these technologies requires continuous investments and strategic planning, as well as efficient articulation between different institutions and levels of government. In addition, issues related to privacy, data governance, and inequality in access to technologies also emerge as critical points in the debate on digital public security (Laufs, 2022).

In this way, technological innovation is configured as a structuring axis of contemporary public security, by enhancing the capacity for monitoring, analyzing and preventing crime. However, their effectiveness depends on the way these tools are integrated into institutional strategies and adapted to local specificities, highlighting the need for studies that analyze their application in regional contexts, such as the State of Tocantins.

3.2 CRIME TRIANGLE THEORY AND SITUATIONAL PREVENTION

The contemporary analysis of crime has been strongly guided by situational approaches that privilege the understanding of the immediate conditions that favor the occurrence of crime. In this context, the *Routine Activity Theory*, proposed by Cohen and

Felson (1979), constitutes the foundation of the so-called Crime Triangle, according to which criminal practice results from the convergence, in the same space-time, of three essential elements: a motivated offender, an adequate target (potential victim) and the absence of a capable guardian/place of the crime. This perspective shifts the explanatory focus from structural causes to contextual and operational factors, allowing for more direct interventions in the environment where the crime occurs (Suslov, 2025).

From this theoretical framework, the situational prevention of crime is consolidated, whose central logic consists of the reduction of criminal opportunities through the modification of physical and social environments. This approach seeks to increase the effort required to commit the crime, increase the risk perceived by the offender and reduce the expected rewards, acting directly on the elements of the triangle. In this sense, strategies such as surveillance, access control, and spatial reorganization are used as deterrence and control mechanisms, contributing to the reduction of crime incidence (Suslov, 2025; Moyo, 2019).

The incorporation of security technologies has significantly expanded the scope of situational prevention, especially with regard to strengthening the "capable guardian". Video surveillance systems (CCTV), for example, are widely used as electronic surveillance tools, allowing both the detection and deterrence of criminal behavior. Empirical evidence indicates that these technologies contribute to the reduction of crimes in monitored areas, in addition to helping to identify offenders and produce evidence for investigations and prosecutions (Papale, 2023; Abdullahi et al., 2025).

In addition, the advancement of digital technologies has enabled the development of intelligent crime prevention systems, based on data and algorithms. Within the scope of *Crime Prevention Through Environmental Design* (CPTED), computational tools have been used to support decision-making in urban control centers, allowing more precise interventions in areas of greater risk. These systems integrate spatial and temporal data to identify patterns and guide preventive strategies, reinforcing the logic of situational prevention and the proactive action of security forces (Choi; Na; Lee, 2024).

In the context of smart cities, crime prevention is mediated by a complex technological infrastructure, which combines urban sensors, digital platforms, and large-scale data analysis. Tools based on data mining and spatio-temporal analysis allow identifying crime patterns and detecting anomalies, subsidizing more effective preventive actions. In this sense, solutions such as continuous monitoring systems and automated alerts contribute to the anticipation of criminal events and the more efficient allocation of police resources (Isafiade; Bagula, 2020; Leal; Gomes-Jr., 2022).

In addition, social participation mediated by digital technologies has emerged as a complementary element in situational prevention. Collaborative platforms and security applications allow the sharing of information between citizens and institutions, expanding the surveillance network and strengthening informal control. This model, often associated with the concept of "digital neighborhood", contributes to the construction of safer environments through cooperation between social and technological actors (Kadar et al., 2016; Ogbu; Excellence, 2025).

On the other hand, the literature also shows that the effectiveness of security technologies in crime prevention is not uniform, being conditioned by factors such as infrastructure, institutional integration and operational capacity. Studies indicate that the simple installation of surveillance systems does not guarantee the reduction of crime, and there may be a displacement of crime to unmonitored areas or limitations in the effective use of technologies. In addition, challenges related to data management, system interoperability, and professional training still represent significant obstacles to the full implementation of these strategies (Mihale-Wilson; Felka; Hinz, 2019; Laufs, 2022).

In this scenario, *data-driven policing* emerges as a complementary approach to situational prevention, by integrating data analysis and operational practices. The use of real-time information and patterns identified in criminal databases allows for a more strategic and efficient performance of police teams, redefining the role of the security agent as a risk manager and information analyst. This integration between technology and police practice reinforces the institutional capacity to intervene in the elements of the Crime Triangle in a more assertive way (Drenth; Van Steden, 2020).

Finally, the literature shows that situational prevention mediated by security technologies represents a promising strategy for reducing crime, by acting directly on the conditions that enable crime. However, its effectiveness depends on the articulation between different technologies, institutional actors, and local contexts, especially in urban environments characterized by structural inequalities. Thus, the Crime Triangle Theory provides a robust analytical framework to understand how these technologies contribute to the disruption of criminal opportunities, guiding their application in specific contexts, such as that of Brazilian cities and, particularly, of the State of Tocantins (Hamada; Nassif, 2018; Laufs; Borrion; Bradford, 2020).

3.3 SURVEILLANCE AND SOCIAL CONTROL TECHNOLOGIES

The advancement of digital technologies has promoted a structural reconfiguration of public security strategies, especially in the mechanisms of surveillance and social control.

Surveillance, previously centered on face-to-face practices, now incorporates technological systems capable of monitoring, recording and analyzing data in real time and on a large scale. This movement is directly associated with the development of smart cities, in which the integration between technological infrastructure and urban management enhances operational efficiency and strengthens crime prevention strategies (Hamada; Nassif, 2018; Ishaphiad; Bagula, 2020).

Among the surveillance technologies applied to public security, video surveillance systems (CCTV) stand out as central instruments in the control of urban spaces. These systems enable the continuous monitoring of strategic areas, expanding the capacity to detect occurrences, the operational response and the production of evidence for investigation. Empirical evidence indicates that CCTV contributes to the deterrence of criminal behavior, especially in property crimes, by increasing the risk perceived by the offender, although its effects are conditioned by the context of implementation and integration with other security strategies (Abdullahi et al., 2025; Moyo, 2019; Papale, 2023).

In addition to video surveillance, intelligent technologies based on artificial intelligence and data mining have expanded social control through automated information analysis. These systems make it possible to identify criminal patterns, detect anomalies, and anticipate occurrences, favoring a more proactive and data-driven action. The integration of spatial and temporal data allows for the continuous monitoring of criminal dynamics and subsidizes strategic decisions in command and control centers, increasing the efficiency of police interventions (Choi; Na; Lee, 2024; Leal; Gomes-Jr., 2022).

In this context, surveillance is mediated by digital networks that expand social participation in the control of security. Collaborative applications and platforms enable the sharing of information between citizens and institutions, configuring forms of distributed and decentralized surveillance. This model, associated with the concept of "digital neighborhood", strengthens informal control and expands the perception of security, while intensifying the continuous monitoring of urban spaces (Kadar et al., 2016; Ogbu; Excellence, 2025).

In the context of smart cities, the integration of surveillance technologies has structured security ecosystems based on the articulation between urban sensors, smart lighting and digital platforms. This technological convergence expands the monitoring and response capacity, allowing for faster and more targeted interventions. Connected infrastructures, such as smart lighting systems, act preventively by changing environmental conditions and reducing criminal opportunities, reinforcing the logic of situational prevention (Mihale-Wilson; Felka; Hinz, 2019; Laufs; Borrion; Bradford, 2020).

On the other hand, the expansion of these technologies intensifies debates about social control, privacy, and data governance. Large-scale monitoring can result in excessive surveillance practices, with impacts on individual rights and civil liberties. In addition, the centralization of data and the use of algorithms in decision-making raise issues related to transparency, *accountability* , and analytical biases, highlighting the need to balance technological efficiency and ethical guarantees in the management of public security (Laufs, 2022).

Another relevant aspect refers to the effectiveness of these technologies in the practice of public security. Although there is evidence of its contribution to crime prevention, its results depend on factors such as territorial coverage, integration between systems, and operational capacity of institutions. The absence of technological coordination and insufficient professional qualification tend to limit their performance, reducing the expected impact on the reduction of crime (Drenth; Van Steden, 2020; Abdullahi et al., 2025).

In this sense, surveillance technologies are central instruments in the restructuring of social control and crime prevention strategies, by expanding monitoring, analysis and intervention capacities. However, its effectiveness is conditioned to the integration between technology, management and institutional context, requiring approaches that articulate technical and social dimensions. From this perspective, the Crime Triangle Theory offers a relevant analytical framework to understand how these technologies act in the reorganization of the conditions that favor crime, especially in regional contexts such as the State of Tocantins.

3.4 CONTEXT OF PUBLIC SECURITY IN TOCANTINS AND THE USE OF SMART TECHNOLOGY IN PREVENTION

The analysis of public security in Brazil shows a scenario marked by regional inequalities, heterogeneous criminal dynamics and persistent structural challenges, which demand strategies adapted to local specificities. Recent data indicate that, although there is a downward trend in some indicators of lethal violence, crime remains high in several regions, with emphasis on property crimes, violence against vulnerable groups, and the growth of crimes associated with the use of technologies, such as fraud and cybercrime. In this context, the adoption of technological tools has been consolidated as a relevant strategy to improve the monitoring, prevention, and response capacity of public security institutions (FBSP, 2025).

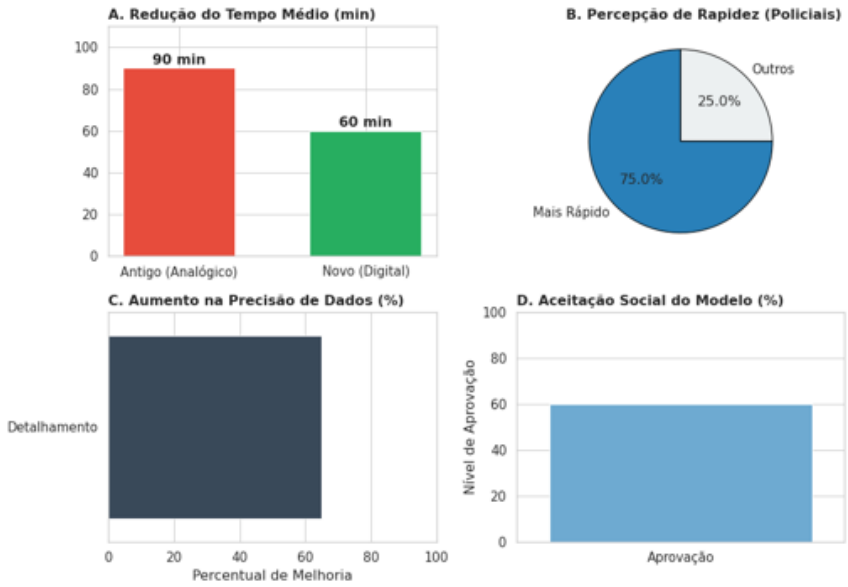
Within the State of Tocantins, public security has its own characteristics, influenced by factors such as recent urban expansion, territorial configuration and the need for integration between different municipalities and regions. In this scenario, the Military Police of the State

of Tocantins (PMTO) has sought to incorporate information and communication technologies as a way to optimize response to occurrences and improve operational efficiency. The implementation of digital systems and mobile applications represents a significant advance in the modernization of the police service, allowing greater agility in the registration of occurrences, data integration, and real-time communication between teams in the field and command centers (Ferreira et al., 2022).

The adoption of the PMTO Mobile system is a concrete example of this technological transformation, by enabling the digital registration of occurrences directly at the scene of the fact, immediate consultation of databases and the reduction of response time to the demands of the population. This tool contributes to improving the quality of the service provided, while strengthening the preventive action capacity of police teams. Studies indicate that the use of this type of technology results in greater operational efficiency, reduction of failures in the recording of information and better management of available resources, evidencing its potential as an instrument to support crime prevention (Tavares; Fernandes; Oliveira, 2023), as shown in Figure 2.

Figure 2

Impact of PMTO Mobile implementation on operational efficiency and security perception



Source: Adapted from (Ferreira et al., 2022; Tavares; Fernandes; Oliveira, 2023).

The results presented indicate consistent gains associated with the adoption of digital technologies in public security. Initially, there was a significant reduction in the average service time, from 90 minutes in the analog model to 60 minutes in the digital model, evidencing greater operational efficiency and speed in responding to incidents. This

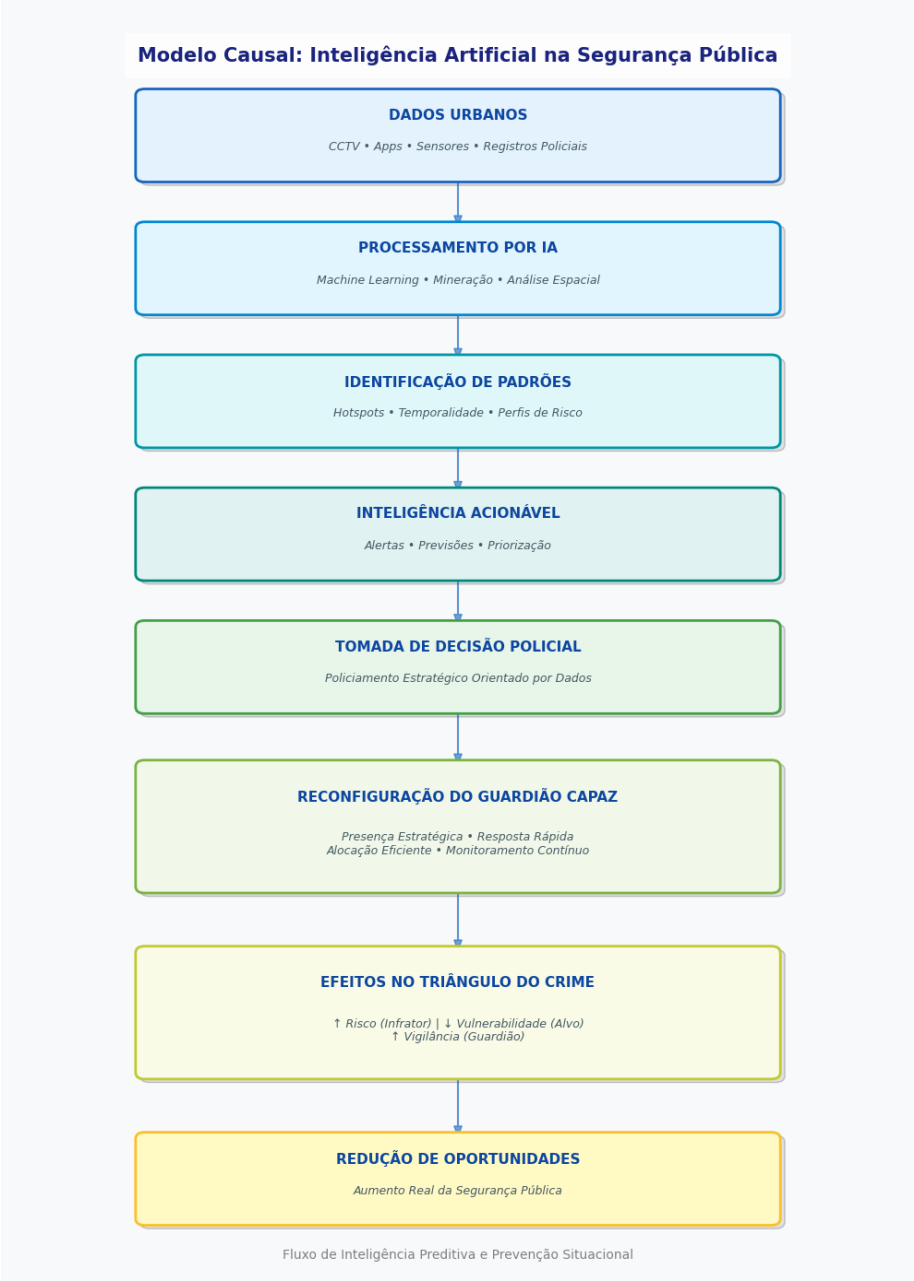
performance is corroborated by the perception of the police officers themselves, of whom 75% consider the service faster after the implementation of the technologies. In addition, there is a significant increase in data accuracy, with an approximate improvement of 65%, reflecting a higher quality of information used in decision-making and reinforcing the data-driven policing model. In the social sphere, the acceptance of the model is also relevant, with about 60% approval, indicating that the incorporation of these technologies contributes to the strengthening of institutional trust. Taken together, these results show that digitalization enhances the performance of the "capable guardian" by increasing the efficiency, analytical capacity, and effectiveness of police interventions (Ferreira et al., 2022; Tavares; Fernandes; Oliveira, 2023).

In this regard, it is verified that in addition to operational applications, the digitalization of administrative processes in police institutions has also contributed to the modernization of public management and to the strengthening of governance in public security. The implementation of electronic protocol and document processing systems allows for greater transparency, agility and accessibility to services, facilitating citizen service and the internal organization of corporations. These initiatives reflect a broader trend of digital transformation in the public sector, in which technology acts as a central element in improving efficiency and scaling institutional capacity (Miranda et al., 2020).

In the context of smart cities, the use of security technologies in Tocantins should be understood as part of a broader process of integration between data, urban infrastructure, and public management. Monitoring systems, mobile applications, and digital platforms contribute to the construction of a more dynamic and responsive security ecosystem, in which real-time information becomes a strategic resource for decision-making. This perspective is in line with the literature that highlights the role of smart technologies in the reorganization of crime prevention strategies, by allowing for more precise and evidence-based interventions (Isafiade; Bagula, 2020; Laufs; Borrion; Bradford, 2020), as shown in figure 3.

Figure 3

Causal model of the reconfiguration of the "capable guardian" based on the use of artificial intelligence in public security



Source: The authors (2026).

However, despite the advances observed, the implementation of security technologies in Tocantins still faces challenges related to infrastructure, systems integration, and human resources training. The effectiveness of these tools depends not only on their availability, but also on the institutional capacity to use them strategically and integrated with public security policies. In addition, the inequality in the distribution of technological resources between different regions can limit the reach of these initiatives, reinforcing the need for continuous planning and investment (Laufs, 2022).

From the perspective of the Crime Triangle Theory, the use of intelligent technologies in Tocantins can be understood as a mechanism to strengthen the "capable guardian", by expanding the surveillance and response capacity of the security forces. At the same time, these technologies contribute to reducing the vulnerability of the targets and increasing the risk perceived by the offender, acting directly in breaking the conditions that favor the occurrence of the crime. Thus, the integration between technology and police strategy is a fundamental element in the construction of more effective prevention policies (Choi; Na; Lee, 2024; Abdullahi et al., 2025).

In addition, the use of digital platforms and collaborative systems expands social participation in the public security process, allowing the sharing of information and the strengthening of informal control. This dynamic contributes to the construction of safer environments, by integrating citizens and institutions into surveillance and cooperation networks. However, it also raises important issues related to privacy, data protection, and governance, which should be considered in the formulation and implementation of these policies (Kadar et al., 2016; Ogbu; Excellence, 2025).

Finally, it is observed that the context of public security in Tocantins shows a transition scenario, in which the incorporation of smart technologies represents an opportunity to improve crime prevention strategies. However, its effectiveness is conditioned to the integration between technology, management and social context, reinforcing the need for approaches that consider both technical and institutional aspects. Thus, the analysis of the use of these technologies in the light of the Crime Triangle Theory allows us to understand in a more in-depth way their impacts on criminal dynamics, contributing to the development of more efficient public policies adapted to the local reality.

4 RESULTS AND DISCUSSION

The analysis of the selected studies, based on Bardin's content matrix, showed that security technologies act differently on the elements of the Crime Triangle, with a significant predominance of interventions aimed at strengthening the "capable guardian". Video surveillance systems (CCTV), digital applications and data-driven policing platforms were identified as the main technological mechanisms used to expand the surveillance and response capacity of security institutions. Empirical studies show that the presence of surveillance cameras contributes to the deterrence of crimes and the production of evidence, reinforcing the perception of risk by the offender and reducing the incidence of crimes in monitored areas (Moyo, 2019; Papale, 2023; Abdullahi et al., 2025).

The integration of smart technologies, such as systems based on artificial intelligence and data mining, has also stood out as a relevant advance in crime prevention, especially in supporting decision-making in command and control centers. These systems allow the identification of criminal patterns and the anticipation of occurrences, promoting a more proactive performance of security forces. In this context, the articulation between data and police practice strengthens the evidence-driven policing model, increasing operational efficiency and the capacity for strategic intervention (Isafiade; Bagula, 2020; Leal; Gomes-Jr., 2022; Choi; Na; Lee, 2024;).

Regarding the "appropriate target" element, the results indicate that technologies such as collaborative applications and urban monitoring systems contribute to reducing the vulnerability of victims, by enabling the sharing of information in real time and the strengthening of informal control. The so-called distributed surveillance, mediated by digital platforms, expands social participation in public security, creating cooperation networks between citizens and institutions. This model, while promising, also entails challenges related to privacy and data governance, requiring regulatory mechanisms that ensure the ethical use of these technologies (Kadar et al., 2016; Ogbu; Excellence, 2025).

Regarding the "motivated offender", it was observed that the use of technologies based on data analysis and artificial intelligence allows not only the identification of criminal patterns, but also the anticipation of criminal behavior. Data mining and spatio-temporal analysis tools contribute to the identification of risk areas and to the more efficient allocation of police resources, acting in a preventive manner to reduce criminal opportunities. In this sense, technology does not eliminate the offender's motivation, but acts to modify the environment, increasing the perceived risk and reducing the chances of success of the criminal action (Isafiade; Bagula, 2020; Leal; Gomes-Jr., 2022).

The literature also shows that the effectiveness of security technologies is directly related to their integration with the institutional structure and the context of application. Although there is consensus on the potential of these tools, several authors highlight limitations associated with infrastructure, system interoperability, and professional training. The lack of integration between different technologies and the inappropriate use of systems can compromise their effectiveness, resulting in limited impacts on crime reduction or even on the spatial displacement of crime (Laufs, 2022; Mihale-Wilson; Felka; Hinz, 2019).

In the Brazilian context and, specifically, in the State of Tocantins, the results indicate that the adoption of digital technologies by police institutions has contributed to the modernization of public security and to the improvement of operational efficiency. The use of institutional applications, such as PMTO Mobile, highlights the potential of mobile

technologies to improve police service, data integration, and reduce response time to incidents. This technological transformation reinforces the role of the "capable guardian", by expanding the institutional presence in the territory and strengthening the capacity for preventive intervention (Ferreira et al., 2022; Tavares; Fernandes; Oliveira, 2023).

In addition, the digitization of administrative processes and the incorporation of electronic systems in police organizations contribute to strengthening governance and transparency in the management of public security. These initiatives reflect a broader trend of digital transformation in the public sector, in which technology acts as a structuring element in improving institutional efficiency and expanding the State's response capacity (Miranda et al., 2020).

However, the integrated analysis of the studies shows that technology, by itself, does not constitute a sufficient solution for reducing crime. Its effectiveness depends on factors such as strategic planning, institutional integration, and adaptation to local specificities. In the case of Tocantins, challenges related to infrastructure, unequal distribution of technological resources, and professional training still represent important limitations for the consolidation of a fully data-driven public security model (Hamada; Nassif, 2018; Laufs, 2022; Tavares; Fernandes; Oliveira, 2023).

Finally, the theoretical and empirical triangulation of the results confirms that security technologies play a fundamental role in breaking the Crime Triangle, by acting simultaneously on its three elements. By strengthening the guardian, reducing the vulnerability of the target, and increasing the risk perceived by the offender, these tools contribute to the reduction of criminal opportunities and the construction of safer environments. However, its effectiveness is conditioned by the integration between technology, management, and social context, highlighting the need for systemic approaches adapted to the local reality, especially in emerging contexts such as the State of Tocantins (Suslov, 2025; Laufs; Borrion; Bradford, 2020; FBSP, 2025).

5 FINAL CONSIDERATIONS

It is concluded that these technologies, especially video surveillance systems and digital applications, act significantly in the reconfiguration of the conditions that favor the occurrence of crime, contributing to the strengthening of the "capable guardian", the reduction of the vulnerability of the "appropriate target" (victim) and the increase in the risk perceived by the "motivated offender". Thus, it is confirmed that the incorporation of technologies in the field of public security constitutes a relevant mechanism for breaking criminal opportunities, especially when integrated with situational prevention strategies.

The main findings indicate that security technologies have a greater impact on strengthening surveillance and expanding the response capacity of police institutions, especially through the use of CCTV, intelligent systems, and operational applications, such as PMTO Mobile. In addition, it was found that data-driven tools and artificial intelligence contribute to the anticipation of criminal patterns and strategic decision-making, while collaborative technologies expand social control and citizen participation. However, the analysis also revealed that the effectiveness of these technologies depends on structural factors, such as systems integration, institutional capacity, professional qualification, and data governance, showing that their adoption alone does not guarantee a reduction in crime.

In view of these results, it is recommended to strengthen public policies that promote the integration between technologies, management and social context, with investments in infrastructure, professional training and interoperability of systems. It is also suggested the development of data-driven public security models adapted to regional specificities, such as in the State of Tocantins, as well as the adoption of governance mechanisms that ensure the ethical and transparent use of technologies. Finally, the need for future research that empirically explores the relationship between security technologies and crime reduction in different territorial contexts is highlighted, contributing to the theoretical and practical advancement of the field of public security.

REFERENCES

Abdullahi, H. G., Sabitu, M., Musa, A. U., & Abubakar, A. S. (2025). The effectiveness and challenges of CCTV camera in crime prevention and control in Kano metropolis, Nigeria. International Journal of Multidisciplinary Research and Growth Evaluation, 6(5), 255–264.

Choi, W., Na, J., & Lee, S. (2024). Evaluating intelligent CPTED systems to support crime prevention decision-making in municipal control centers. Applied Sciences, 14, 6581. https://doi.org/10.3390/app14156581

Drenth, A. R., & van Steden, R. (2020). Everyday patrol work for a data-driven flying squad: advancing theoretical thinking on police craftsmanship in interacting with civilians. Journal of Crime and Justice, 43(4), 486–501. https://doi.org/10.1080/0735648X.2020.1722202

Ferreira, L. M. S. C. B., Almeida, J. T. V., Santos, W. R., & Barbosa, W. G. (2022). PMTO Mobile e sua contribuição tecnológica no atendimento de ocorrências policiais. Revista Brasileira de Segurança Pública (RIBSP), 5(12). https://doi.org/10.36776/ribsp.v5i12.181

Fórum Brasileiro de Segurança Pública. (2025). 19º anuário brasileiro de segurança pública. São Paulo: Fórum Brasileiro de Segurança Pública.

Hamada, H. H., & Nassif, L. N. (2018). Perspectivas da segurança pública no contexto de smart cities: desafios e oportunidades para as organizações policiais. Perspectivas em Políticas Públicas, 11(22), 155–179.

Isafiade, O. E., & Bagula, A. B. (2020). Series mining for public safety advancement in emerging smart cities. Future Generation Computer Systems, 108, 777–802. https://doi.org/10.1016/j.future.2020.03.002

Kadar, C., Te, Y.-F., Brüngger, R. R., & Cvijikj, I. P. (2016). Digital neighborhood watch: to share or not to share? In Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems. New York: ACM. http://dx.doi.org/10.1145/2851581.2892400

Laufs, J. (2022). Crime prevention and detection technologies in smart cities: opportunities and challenges (Tese de doutorado). University College London.

Laufs, J., Borrion, H., & Bradford, B. (2020). Segurança e cidade inteligente: uma revisão sistemática. Sustainable Cities and Society, 55, 102023. https://doi.org/10.1016/j.scs.2020.102023

Leal, M. F., & Gomes-Jr., L. (2022). CityGuardian: uma ferramenta para monitorar mudanças em padrões de criminalidade nas cidades inteligentes. In Anais estendidos do XVIII Simpósio Brasileiro de Sistemas de Informação (SBSI 2022).

Lujas, J., Borrion, H., & Bradford, B. (2020). Segurança e cidade inteligente: uma revisão sistemática. Sustainable Cities and Society, 55, 102023. https://doi.org/10.1016/j.scs.2020.102023

Mihale-Wilson, C., Felka, P., & Hinz, O. (2019). The bright and the dark side of smart lights: the protective effect of smart city infrastructures. In Proceedings of the 52nd Hawaii International Conference on System Sciences (pp. 3345–3354).

Miranda, D. M., Rezende, J. A. B., Tossatti, R. G., & Faneli, T. R. (2020). Implementação de sistema de protocolo digital nas polícias militares da Bahia, Rondônia e Tocantins.

Moyo, S. (2019). Evaluating the use of CCTV surveillance systems for crime control and prevention: selected case studies from Johannesburg and Tshwane, Gauteng (Dissertação de mestrado). University of South Africa.

Ogbu, M. N. C., & Excellence, D. F. (2025). Leveraging information and communication technology for enhancing crime prevention and safety in Nigerian universities. Caritas Journal of Engineering Technology, 4(2).

Papale, P. (2023). The role and impact of CCTV operators in contributing to efficient crime prevention: a case study of surveillance operators within the City of Cape Town (Dissertação de mestrado). University of Cape Town.

Suslov, T. (2025). Prevenção do crime. In Repensando a segurança pública: prevenção do crime e gestão da segurança. Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-031-92068-4_9

Tavares, L. F. S., Fernandes, J. A. F., & Oliveira, C. J. (2023). A implementação da tecnologia PMTO Mobile: vantagens x desvantagens. Revista Brasileira de Segurança Pública (RIBSP), 6(14). https://doi.org/10.36776/ribsp.v6i14.180