UNIVERSITÀ DEGLI STUDI DI PADOVA

SCIENZE POLITICHE, GIURIDICHE E STUDI INTERNAZIONALI (SPGI)

Master's Degree Course in European and Global Studies

The Role of Surveillance Technologies in Brazil's Public Security: Addressing Legal and Ethical Concerns

Supervisor:
Professor Guido Gorgoni

Candidate: Luiza Storino Cavalcanti
Student ID number: 2041145

Academic Year
2022/2023

À minha torcida

ACKNOWLEDGEMENT | AGRADECIMENTOS

Agradeço a Deus por ter me proporcionado todas as oportunidades, tendo sido a mão que me guiava e apoiava para que em nenhuma pedra eu tropeçasse durante esse árduo caminho, sendo meu refúgio e alegria com tamanho amor e misericórdia.

Agradeço à minha família, Flávia, Gil e Clara, por ser a minha base sólida a partir da qual posso me desenvolver, pois tenho o amor como porto-seguro e bons valores como meu norte. Obrigada pelo apoio à minha decisão de cruzar o Oceano, apesar da saudade. Obrigada por terem acreditado em mim quando nem eu mesmo fui capaz.

Agradeço a minha mãe, pelo amor incondicional e sua presença desde meu primeiro choro no mundo até as madrugadas estudando para provas, por ser símbolo de garra e cuidado, inteligência e determinação, sendo fonte inspiradora para que haja cada uma destas qualidades em meus feitos.

Agradeço ao meu pai, cuja dedicação foi fundamental para viabilizar meu percurso acadêmico, e cujas palavras proferidas serviram como farol em minha jornada, iluminando os caminhos, e me ensinaram sobre o amor, o poder da fé e a importância da resiliência.

Agradeço a minha irmã, a quem não chamo só de irmã, mas de parceira de vida, por ser a minha maior torcedora e a fonte profunda da minha crença em mim mesma, a força motriz da minha motivação para lutar pelo sucesso, tornando as minhas aspirações uma realidade.

Agradeço a cada membro da minha família, em especial, ao meu padrinho Alessandro e a minha tia Dani pela preocupação e constante carinho; e ao Vô Geraldo e a Vó Cilene, pelo apoio, afeto e motivação.

Agradeço ao José pela influência positiva com suas melhores qualidades, por fazer dar certo, por ter me apresentado um mundo de possibilidades, pelo amor e infinitas memórias.

Agradeço aos meus grandes amigos, Mateus, Maria, Rick, Lorena, Evandro, Júlia, Yasmin, Isabela, Luisa, Juliana, Lucas Felipe, Letícia, Márcia, e aos amigos de Padova, que viraram minha segunda família, pelo suporte e pelos momentos inesquecíveis.

Agradeço ao meu orientador, Professor Guido Gorgoni, pela disponibilidade e tamanha gentileza durante todo o processo; e ao querido Professor Ricardo Oliveira, que é exemplo de compaixão e sapiência.

Agradeço, *in memoriam*, aos meus antepassados as quais jornadas permitiram que eu chegasse até aqui, em especial a minha amada Vó Lúcia, por tanto carinho, amor e incentivo, por ter me prestigiado em todos os momentos e pelo orgulho de cada um dos meus pequenos avanços, tenho certeza de que não seria diferente agora.

Only “we the people” can reverse this course, first by naming the unprecedented, then by mobilizing new forms of collaborative action: the crucial friction that reasserts the primacy of a flourishing human future as the foundation of our information civilization.

(Zuboff, 2019)

ABSTRACT

As the Fourth Industrial Revolution unfolds, intertwining technological advancements with societal fabric, the captivating exploration of surveillance technologies within public security unfolds as a multifaceted and interdisciplinary investigation, scrutinizing contemporary society through the intersecting lenses of governance, politics, law, and rights. The study delves into the profound relevance of cutting-edge tools such as artificial intelligence, data analytics, and interconnected systems for the empowerment of unprecedented surveillance capabilities, under public security context. In this manner, the overarching goal of this research is to comprehensively investigate the intricate relationship in Brazil, a nation susceptible to testing emerging trends and widespread deployment of such technologies. Employing a qualitative methodology through an exploratory approach, the study takes into account their historical evolution, integration processes, and the legal and ethical dimensions that accompany their deployment. Starting from a solid theoretical framework that emphasizes the parallels between modern surveillance techniques and power dynamics with the contemporary character, it analyzes ongoing surveillance-based projects and models towards public security through Brazilian territory. Revealing the imperative for a nuanced balance between public safety imperatives and the protection of individual rights, the study identifies technological limitations, particularly errors in facial recognition, and emphasizes the risks of algorithmic biases, especially in a racially diverse society like Brazil. It addresses the existing legal gap in data protection laws related to public security and criminal investigation, advocating for a comprehensive regulatory framework that safeguards fundamental rights. In conclusion, the research not only broadens the understanding of historical, ethical, and legal dimensions but also underscores the significance of a balanced and informed approach in deploying and regulating surveillance tools. The findings pave the way for further studies on public security policies, operational efficiency, innovation, and the protection of fundamental rights, revealing promising avenues for future research and discourse in contemporary society.

Keywords

Surveillance; Public Security; Algorithmic Biases; Legality, Ethics.

SUMMARY

Introduction

The trajectory of humanity is a narrative interlinked with innovation, progress, and societal transformation. Societal morphology is correlated to a transformative technological development, rooted in the centrality of knowledge that enables information and communication capacity to evolve. The penetration of technologies into human activities is a starting point to analyze the complexities involved in politics, economy, culture, and security. Still, it is important to note a co-constitutive manner in this relationship, which means that there exists an interactive pattern between technology and society. As Castell (2000) notes:

> "Yet, if society does not determine technology, it can, mainly through the state, suffocate its development. Or alternatively, again mainly by state intervention, it can embark on an accelerated process of technological modernization able to change the fate of economies, military power, and social well-being in a few years. Indeed, the ability or inability of societies to master technology, and particularly technologies that are strategically decisive in each historical period, largely shapes their destiny, to the point where we could say that while technology per se does not determine historical evolution and social change, technology (or the lack of it) embodies the capacity of societies to transform themselves, as well as the uses to which societies, always in a conflictive process, decide to put their technological potential" (Castells, 2010, p. 7).

The novel social structure is intricately linked to the emergence of a new mode of development, which is shaped by the restructuring of the capitalist mode of production, particularly as it unfolded towards the conclusion of the twentieth century (Castells, 2010, p.14). In this new mode of development entitled "informational", productivity emanates from the technology of knowledge generation, information processing, and symbol communication, which means that knowledge itself is the primary source of productivity (Castells, 2010).

Among the information technologies, Castells (2010, p.29) identifies "set of technologies in micro-electronics, computing (machines and software), telecommunications/broadcasting, and opto-electronics", besides "genetic engineering and its expanding set of developments and applications". Thus, Artificial Intelligence (AI), Big Data, and the Internet of Things (IOT) are framed in this context.

In line with Castells (2010), those digital developments and technologies are foundations for the "Fourth Industrial Revolution", conceptualized by Schwab (2016, p.12), which denotes a profound shift that frames the current scenario. The fusion of all these technologies and the interconnection between "physical, digital and biological" spheres differentiates this revolution from the others (Schwab, 2016, p.12). Moreover, Castells (2010, p.30) notes that the current technological revolution is characterized by technologies of information processing and communication:

> "What characterizes the current technological revolution is not the centrality of knowledge and information, but the application of such knowledge and information to knowledge generation and information processing/communication devices, in a cumulative feedback loop between innovation and the uses of innovation" (Castells, 2010, p. 31).

Technology, with its emphasis on knowledge acquisition through data production, and processing, becomes pivotal in this field. Once data production is facilitated, information gathering about daily activities, behaviors, physical characteristics and so on were intensified through surveillance methods. The omnipresence of digital devices in all spheres of human life is a fruitful ground for unprecedented occurrences in diverse spheres, being social, political, economic. In this context of emergence of "electronic text' and spread of "computer mediation", Shoshana Zubbof (2015, p. 77) affirms that "nearly every aspect of the world is rendered in a new symbolic dimension as events, objects, processes, and people become visible, knowable, and shareable in a new way"[1].

Thus, data gathering is the sustenance of "machine intelligence", which refers to the ability of machines or computer systems to 'learn' and make decisions on their own based on the data they receive (Zuboff, 2019, p.14). Thus, the intense influx of data allows the improvement of performance in terms of patterns, trends, and anomalies detection, thus, feeds the accuracy of the prediction[2] (Zuboff, 2019; O'Neil, 2016).

In this digital information society, systematic surveillance activities have become pervasive. Notably, social media platforms have developed systems capable of analyzing users' profiles and consumption patterns. This capability allows companies to gain valuable insights into consumer behavior, enabling them to tailor marketing strategies accordingly[3]. The expanded scope of surveillance has permeated diverse sectors, impacting various activities. In the field of human resources, these applications are utilized for selection process for job application and work schedules[4]. Similarly, in the realm of education, they play a crucial role in ranking and admission processes. Additionally, they extend their influence into determining

[1] Zuboff (2015, p.77) writes that "the world is reborn as data and the electronic text is universal in scale and scope".

[2] Zuboff (2019, p.14) affirms that "data are applied to product or service improvement, (...) and fabricated into prediction products that anticipate what you will do now, soon, and later". Following this sense, Cathy O'Neil (2016, p. 173) points out that "Big Data processes codify the past.". Due to prediction objetive, "continuously improving the system" means closing the gap between prediction and observation in order to approximate certainty" (Zuboff, 2019, p.190).

[3] Under the 'Surveillance Capitalism' thematic, Shoshanna Zuboff (2015, p.5) defends a 'new approach' that "depended upon the acquisition of user data as the raw material for proprietary analyses and algorithm production that could sell and target advertising through a unique auction model with ever more precision and success"

[4] In 'Weapons of Math Destruction', Cathy O'Neil (2016, p. 16) argus that "an algorithm processes slew of statistics and comes up with a probability that a certain person might be a bad hire, a risky borrower, a terrorist, or a miserable teacher. That probability is distilled into a score".

eligibility for credit cards, loans[5], and insurance policies[6]. Finally, the public sector employs surveillance for various purposes, including crime prevention and public safety[7].

Those diverse forms of surveillance are shaping various facets of contemporary society, emphasized by their intricate coexistence governmental and private spheres[8], and giving rise to new challenges and intricate situations that necessitate comprehensive understanding and addressing within the mentioned fields (Bordignon, 2020). Notably, these two dimensions cooperate and mutually reinforce each other, giving rise to unprecedented scenarios in the realms of governance, control, democracy, rights, policies, urban organization, and so on[9] (Bordignon, 2020).

Under these distinguishing features of pervasive ubiquity, immense power, and widespread accessibility of technologies, surveillance practices were facilitated, expanded and intensified. Frequently, these activities brought to light previously obscured aspects, or better, it was revealed. Knowledge on such practices was initially transpired through disclosures by former employees of significant technology firms and government intelligence centers. For instance, the reference to Edward Snowden's revelations in 2013 about the global surveillance scheme of the United States' National Security Agency (NSA) serves as an illustrative example

[5] In *The Age of Surveillance Capitalism* book, Zuboff (2019, p. 247) utilizes the case of China to clarify about credit process within this new dynamic that utilizes surveillance, data gathering and analysis, additionally, the author says that "when it comes to credit scoring, US and UK banks and financial services firms have floated business models based on the mining and analysis of social media data for credit scores"

[6] "Insurers can eliminate uncertainty by shaping behavior. The idea is to continuously optimize the insurance rate based on monitoring the driver's adherence to behavioral parameters defined by the insurer" (Zuboff, 2019, p. 141). For instance, "Wearable accelerometers" could "improve traceability of their compliance" with prescribed exercise regimes, and "digestible sensors" could track compliance with dietary and medication schedules, "providing higher truth and better granularity than a monthly refill." (Zuboff, 2019, p. 141)

[7] Badin & Viana (2022, p.7, translated by the author) says that "the information civilization does not limit only changes in the area of capital accumulation: they are increasingly served by state surveillance".

[8] Bordignon (2020) suggests that surveillance transcends a simple shift from the public/governmental to the private/corporate spheres, as some other authors defend.

[9] "Some authors, such as Leal (1996), even formulate the ethical challenges of the information society in terms of a multiple loss: loss of qualification, associated with automation, and unemployment; interpersonal and group and group communication, transformed by new technologies or even destroyed destroyed by them; of privacy, due to the invasion of our individual individual space and the effects of visual violence and of control over our personal lives and the world around us surrounding world; and a sense of identity, associated with the intimidation by the growing complexity" (Werthein, 2000, p.75, translated by the author).

of governmental surveillance (Zuboff, 2015; Schwab, 2016; Bordignon, 2020; Badin & Viana, 2022). This concrete example reveals an existing scheme of surveillance under governmental scrutiny, highlighting the potential for abuses of power, raising concerns about rights and the need for transparency in surveillance activities.

Those experiences of information societies, as mentioned earlier, emphasizes the understanding of the dynamic relationship between economic changes, technological advancements, state intervention, and their impact on the local social fabric. Thusly, it is possible to perceive a spread of new information technologies led and mediated by the State (Werthein, 2000).

The increasing reliance of the public sector on technology for gathering personal data is driven by the objective of advancing public policies, aiming to enhance the efficiency of public resources and broaden the reach of governmental initiatives. This trend includes the development of applications with integrated databases to facilitate access to public services. However, an extensive collection of personal data emerges, with potential implications for surveillance and control, both by governmental authorities and technology-savvy companies.

Therefore, the array of devices that rely on collection, processing, and leveraging data to manage and regulate various aspects of human lives are described by Bordignon (2020) as “technopolitical devices", which are surveillance and control techniques associated with Information and Communication Technologies (ICTs). In the current dimension of technopolitical surveillance, a distinct panoptic structure is adopted. This metaphorical design, embraced by Foucault to represent modern life, underscores that surveillance constructs a panopticon without physical walls. In contemporary times, facilitated by modern electronic technologies, individuals are watched, yet the identity of those conducting surveillance usually remains concealed, intensifying the panoptic dynamic (Webster, 2006). This digital panopticon generates a continuous sense of being observed, much like perpetual surveillance cameras and similar devices (Han, 2018).

Those concepts are particularly intangled to the implementation of public policies, especially those related to security. The adoption of Information and Communication Technologies (ICTs) for public security policies gained traction in Brazil. Following the establishment of the legal framework for public security as prescribed by the Brazilian Federal Constitution, the integration of surveillance technologies becomes a critical aspect. Shaped by principles such as prevention, justice, and societal reintegration, this integration reflects Brazil's efforts to balance security imperatives.

Measures to promote the modernization of equipment, investigations, and standardization of technology across security entities are commonly identified. The most recent initiative departs from the Plano Nacional de Segurança Pública e Defesa Social 2021-2030, which has a specific focus envisioning the use of technology for the standardization, integration, and interoperability of security-related data at various governmental levels (Plano Nacional de Segurança Pública e Defesa Social 2021-2030, 2021).

The governamental utilization of technology is an effort to develop more intelligence-driven actions to control the exponential growth of violence in Brazil. According to the United Nations Office on Drugs and Crime (UNODC), Brazil holds the highest absolute number of homicides globally and ranks as the eighth most violent country in the world, according to (Fórum Brasileiro de Segurança Pública, 2022).

This approach, employed as a strategy to address criminal activities, has been implemented in various forms in Brazil through the years, particularly in the realm of public policies involving technology. Its approval for utilization in the security sector is marked by a specific endorsement for deploying advanced tools, including but not limited to body-worn cameras, drones, videosurveillance cameras, and technologies such as artificial intelligence (AI), machine learning (ML) facial recognition (FR).

In spite of some positive outcomes presented in the operationalization of public policies, the introduction of technology draws attention to the reconciliation of security and rights, particularly concerning privacy and personal data. Several concerns have emerged and prompted reflections. For instance, the nature of technology could encounter technical limitations affecting accuracy and reliability, thereby impacting the effectiveness of person recognition (O'Neil, 2016; Kitchin, 2014). Those errors could affect individuals on different scales. Associated with algorithms that are incorrectly labeled and biased, the identification of innocent individuals may occur, and particularly affect individuals from minority groups (O'Neil, 2016; Nunes, 2019; da Silva, 2022).

Therefore, it becomes imperative to consider the possibility of technology usage resulting in violations of freedom, privacy, and personal data protection rights (Rodotà, 2009; Solove, 2011). This underlines the crucial role of regulation in adapting and diffusing new technologies. Noteworthy is the existence of the Lei Geral de Proteção de Dados (Lei Geral de Proteção de Dados Pessoais, 2018), the Brazilian General Data Protection Law, emphasizing privacy and data protection. Nevertheless, concerns emerge as its current limitations in addressing issues within the public security sector may reopen a precarious gap in the regulatory structure.

In view of the nuanced and significant theme, especially given its multiplicity of impacts on different scopes of human existence, including the public security sector, this research proves valuable and pertinent. Elucidating risks of implementation through analysis of ethical and legal challenges, it will defund social awareness on the theme. In an epoch characterized by rapid technological progress and heightened societal concerns, it will be responsible to provoke a deeper debate and a profound study, which will create a consolidated basis for the necessary response or appropriate regulatory framework.

The identification of research problems and the underlying motivation stems from the proliferation of surveillance technologies in public security presents a complex sphere with significant implications. As technology enhances the operational capacities of security forces, it intertwines with legal, ethical, and societal dimensions, necessitating an in-depth exploration. This research aims to scrutinize the multifaceted impact of surveillance technologies on Brazil's public security sector, delving into their evolution, integration, and associated legal and ethical complexities. The study addresses the following questions: How have surveillance tools and technologies evolved, and what role do they play in shaping power dynamics within public security? What is the specific influence of surveillance technologies on Brazil's security landscape? What ethical challenges emerge from the use of surveillance technologies in the context of public security? How do legal frameworks in Brazil regulate the deployment and operation of surveillance technologies in the public security domain?

Based on the pressing questions, the overarching goal of this research is to comprehensively investigate the intricate relationship of surveillance technologies and the public security sector in Brazil, taking into account their historical evolution, integration processes, and the legal and ethical dimensions that accompany their deployment. The research seeks to provide a nuanced understanding of the multifaceted role of surveillance tools in shaping power dynamics within public security.

The specific objectives of this research are a) to describe the historical development of surveillance tools and techniques; b) to identify the existing projects and plan on the use of surveillance technologies in the realm of public security in Brazil; c) to investigate potential risks arising from the use of surveillance technologies, assessing implications on fundamental rights and ethical challenges in the context of public security; d)to examine existing legal frameworks in Brazil governing the deployment and operation of surveillance technologies in public security; e) to identify gaps or areas of improvement in the legal frameworks pertaining to surveillance technologies; f) to propose recommendations and improvements based on the analysis of benefits, risks, and ethical considerations. By pursuing these specific objectives, the research aims to contribute valuable insights into the advancing landscape of surveillance technologies in Brazil's public security, fostering a holistic understanding that encompasses technological, ethical, and legal dimensions.

In terms of methodology, to delve further into the meanings, concepts, definitions, characteristics, metaphors, symbols, and descriptions associated with surveillance technologies, public security, and the ethical and legal considerations, this research adopted a qualitative approach (Lune et. Berg, 2017). According to Howard Lune and Bruce L. Berg (2017), qualitative research is characterized by the effort to describe, understand, and explain things.

The chosen exploratory research methodology is particularly apt for this work on surveillance technologies in public security due to the complex and evolving nature of the subject matter. In line with Gil (2002), this type of research aims to provide greater familiarity with the problem, with a view to making it more explicit. It allows a comprehensive understanding of the problem that is multifaceted and rapidly advancing. To foster this familiarity, it was necessary to delve into existing literature, theories, and practical applications, enabling the identification of the key issues, challenges, and opportunities within the realm of this topic. Moreover, the flexibility within this type of research aligns with the dynamicity and amplitude of surveillance technologies, which enables the consideration of varied aspects of the studied fact, in this case, legal, ethical, technical, and social dimensions.

The exploratory research can invoke some techniques, including literature reviews, and the analysis of examples that "stimulate understanding", as noted by Gil (2002, p. 41, translated by the author). In the realm of this research, a literature review was executed by using references of theoretical frameworks, thesis dissertations, scientific articles and journals, and reports. Thus, the analysis of examples helped to contextualize theoretical frameworks within real-world cases, providing valuable insights into how these technologies are implemented, their impact on society, and the associated legal and ethical issues.

With an emphasis on technical data collection and analysis procedures, this work was developed based mainly on books and scientific articles. Additionally, a documentary research was conducted, regarding specifically, laws, directives, regulations, bills, notices.

This research is justified by the pressing need to comprehensively understand the evolving landscape of surveillance technologies in Brazil's public security sector. The increasing integration of these technologies poses complex challenges that extend beyond technological advancements, touching upon ethical, legal, and societal dimensions. By contributing to academic discourse, this study not only advances scholarly understanding but also provides valuable guidance for policymakers, security practitioners, and the public in navigating the complexities of surveillance technologies responsibly. In an era marked by technological advancements and societal concerns, this research serves as a timely and crucial endeavor to inform policies that strike a balance between security imperatives and the protection of fundamental rights in Brazil.

Considering the presented background of an era marked by technological advancements and a growing reliance on surveillance technologies, the intricate relationship between surveillance, public security, and individual rights demands a nuanced exploration. The subsequent organization of this work revolves around three principal chapters, each of which will be elucidated below.

The initial chapter is structured to provide a comprehensive understanding of surveillance discussions. It draws upon Michel Foucault's theoretical framework as a foundation for understanding the power dynamics and its inherent apparatuses in surveillance and its implications on society. Furthermore, by dissecting Foucault's concepts, it explores the broader field of surveillance studies to establish key aspects that shape surveillance in the contemporary world.

Moving beyond theoretical underpinnings, Chapter 2 zooms in on Brazil's security situation, unraveling the intricate relationship between surveillance technologies and public security. The chapter navigates through the evolution of surveillance technologies application in the Brazilian context, providing insight into the motivations and consequences of their integration. A meticulous mapping of the national security panorama highlights the varied applications and implications of surveillance technologies.

Chapter 3 delves into the legal and ethical complexities surrounding the use of surveillance technologies in Brazil's security scope. By scrutinizing the ethical implications of these technologies, the chapter sheds light on the ethical dilemmas posed by the surveillance apparatus. Additionally, it explores the regulatory frameworks governing public surveillance, analyzing the interplay between legal structures and the ethical considerations associated with surveillance technologies.

The concluding section synthesizes the findings from the preceding chapters, offering a holistic understanding of the role and impact of surveillance in the security scenario in Brazil. It reflects on the ethical and legal challenges posed by surveillance technologies and suggests potential avenues for policy and practice. Finally, the bibliography provides a comprehensive list of sources that underpin this exploration, allowing readers to delve deeper into the intricate realm of surveillance studies.

CHAPTER 1

Surveillance discussed

Surveillance is a multifaceted phenomenon at the intersection of power, technology, and societal dynamics, and occupies a central position in contemporary discourse on public security. It is indispensable to explore beyond the superficial gaze, profounding into domains of theoretical frameworks and contemporary studies. Exploring the historical underpinnings and enduring relevance of concepts such as power, discipline, and societal vigilance becomes paramount, which leads to the intellectual groundwork elaborated by Michel Foucault. Building upon that foundation, modern surveillance practices can be better understood. This comprehension will allow moving the attention toward the practical applications of surveillance technologies within the public security sector, examining their impact, particularly in Brazil. This examination will raise important ethical and legal questions, prompting thoughtful discourse and further exploration in this incipient and fastly-moving field.

1.1 Exploring Michel Foucault's theoretical framework on surveillance

In "Discipline and Punish: The Birth of the Prison" (1995), Michel Foucault delves into the metamorphoses of punitive methods by examining societal dynamics related to power relations and political technologies. The transformation of social structure of punishment over time is explored through a genealogical approach[10]. It endeavors to meticulously investigate the subject of study, focusing on its characteristics across different historical periods rather

[10] Hence, observing and examining events unfolding over time without aiming for an origin.

than seeking an origin or essential nature[11]. By carefully analyzing these historical forces, it is perceived a metamorphoses of punitive methods in relation to power dynamics and political technologies, from a focus on physical discipline and public torture to a more subtle, internalized form of control.

From this historicity, the author presents a critical analysis on penal practices. In the past, severe forms of punishment were directed at the body, which is no longer the primary focus. Instead of inflicting physical pain, the aim is to act on a deeper level. The reduction in penal severity has been viewed as synonymous of less cruelty, pain, and more humane treatment[12]. However, the author argues that alongside these changes, there has been a qualitative shift in the very nature of punishment due to a change of objective (Foucault, 1995). There is a shift in the perception and treatment of the body[13], which is the object and target of power, revealing a newfound interest in controlling and shaping its functions, operated in a sophisticated understanding and through a manipulative capacity of the body:

> "This subjection is not only obtained by the instruments of violence or ideology; it can also be direct, physical, pitting force against force, bearing on material elements, and yet without involving violence it may be calculated, organized, technically thought out; *it may be subtle*, make use neither of weapons nor of terror and yet remain of a physical order. That is to say, there may be a 'knowledge' of the body that is not exactly the science of its functioning, and a mastery of its forces that is more than the ability to conquer them: this knowledge and this

[11] Through genealogy, a critical view of the events was performed from the observation of its own unfolding.

[12] "The reduction in penal severity in the last 200 years is a phenomenon with which legal historians are well acquainted. But, for a long time, it has been regarded in an overall way as a quantitative phenomenon: less cruelty, less pain, more kindness, more respect, more 'humanity'. In fact, these changes are accompanied by a displacement in the very object of the punitive operation. Is there a diminution of intensity? Perhaps. There is certainly a change of objective. If the penalty in its most severe forms no longer addresses itself to the body, on what does it lay hold.The answer of the theoreticians - those who, about 1760, opened up a new period that is not yet at an end - is simple, almost obvious. It seems to be contained in the question itself: since it is no longer the body, it must be the soul. The expiation that once rained down upon the body must be replaced by a punishment that acts in depth on the heart, the thoughts, the will, the inclinations. Mably formulated the principle once and for all: 'Punishment, if I may so put it, should strike the soul rather than the body'(Mably, 326)" (Foucault, 1995, p.16)

[13] "The classical age discovered the body as object and target of power. It is easy enough to find signs of the attention then paid to the body - to the body that is manipulated, shaped, trained, which obeys, responds, becomes skilful and increases its forces" (Foucault, 1995, p.136).

> mastery constitute what might be called the *political technology of the body*" (Foucault, 1995, p.26, emphasis added)

For this, methods allowing meticulous control over the body's operations are used, ensuring constant subjection of its forces and establishing a relation of docility-utility[14]. This modality is called "disciplines"[15], which refers to a calculated manipulation of the body's elements, gestures, and behavior, and it is characterized by several key features (Foucault, 1995, p. 137).

> "Discipline may be identified neither with an institution nor with an apparatus; it is a *type of power, a modality for its exercis*e, comprising a whole set of instruments, techniques, procedures, levels of application, targets; it is a 'physics' or an 'anatomy' of power, a technology. And it may be taken over either by 'specialized institutions (the penitentiaries or 'houses of correction' of the nineteenth century) (...), or finally by state apparatuses whose major, if not exclusive, function is to assure that discipline reigns over society as a whole (*the police*)." (Foucault, 1995, p. 215-216, emphasis added)

The modality of discipline encompasses an operation of "uninterrupted and constant coercion", establishing a sustained influence over an individual's actions or behavior. Furthermore, discipline stands out for its focus on supervising processes, monitoring and regulating the methods and processes employed in an activity. Lastly, involves a systematic codification, meticulously organizing and partitioning "time, space, and movement"[16]

[14] "the body that is manipulated, shaped, trained, which obeys, responds, becomes skilful and increases its forces" (Foucault, 1995, p.136).

[15] "These methods, which made possible the meticulous control of the operations of the body, which assured the constant subjection of its forces and imposed upon them a relation of docility-utility, might be called 'disciplines'. Many disciplinary methods had long been in existence - in monasteries, armies, workshops. But in the course of the seventeenth and eighteenth centuries the disciplines became general formulas of domination" (Foucault, 1995, p.137).

[16] "It implies an uninterrupted, constant coercion, supervising the processes of the activity rather than its result and it is exercised according to a codification that partitions as closely as possible time, space, movement. These methods, which made possible the meticulous control of the operations of the body, which assured the constant

(Foucault, 1995, p.137). These fundamental characteristics are pivotal for the examination of surveillance technologies within the public security sector, as will be elaborated upon in the subsequent sections of this work.

In this regard, Foucault (1995) names two concepts of discipline. The first concept, referred to as "discipline-blockade" encompasses the negative functions carried out by institutions located at the margins of society[17] (Foucault, 1995, p. 209). Conversely, the second concept, named "discipline-mechanism", involves the utilization of more subtle methods that exert a positive influence on the exercise of power. The latter form of discipline is designed to enhance the exercise of power by making it "lighter, more rapid, more effective" (Foucault, 1995, p. 209). It represents a strategic approach to coercion, intending to be subtle in its impact on individuals. It envisions a society in which power is exercised with increased efficacy and rapidity, suggesting a forward-looking design for shaping behavior in a more nuanced manner. These mechanisms revolve around generalized surveillance that embraces the entirety of society[18].

In understanding the features of modernity, it is crucial to introduce Foucault's (1995) concept of power. For Foucault (1995), power is a network that is present throughout societal relations, from which emerges systems, processes and institutions that characterize a specific historical conjecture and its rationalities. It has a diffuse character, which means that it is not held, but intrinsically exercised within these relations. Taking this into consideration, it is possible to understand the exercise of power and self-sustainment mechanisms.

subjection of its forces and imposed upon them a relation of docility-utility, might be called 'disciplines'." (Foucault, 1995, p. 137)

[17] "arresting evil, breaking communications, suspending time" (Foucault, 1995, p.209)

[18] "The movement from one project to the other, from a schema o f exceptional discipline to one of generalized surveillance, rests on a historical transformation: the gradual extension of the mechanisms o f discipline throughout the seventeenth and eighteenth centuries, their spread throughout the whole social body, the formation of what might be called in general the disciplinary society." (Foucault, 1995, p.209).

Primarily, the exercise of power of the sovereign through punishment is an essential part of administration, where the ceremonies convey a disportion of power in the social relation between sovereign and population, but especially the subject of punishment (Foucault, 1995) [19]. For instance, public torture exercised this function of force manifestation, a emphatic liturg y for affirmation of power and superiority[20]. Moreover, the embodiment of power, physically and materially, expresses more than the existing power relations, but also makes it possible to clearly identify the perpetrators.

The emergence of a new social political configuration not only signifies a reorganization of human relations within society, but also unveils a transformation in our understanding of spaces and subjectivity[21]. This transformative shift paves the way for the rise of a new disciplinary power, as exposed, influencing the dynamics of our modern world. From physical suffering[22] to an a "system of constraints and privations, obligations and prohibitions"[23] (Foucault, 1995, p.11). The 'technical mutation' represents a shift in power dynamics and marks the emergence of a disciplinary society[24]. This progressively

[19]"The public execution, then, has a juridico-political function. It is a ceremonial by which a momentarily injured sovereignty is reconstituted. It restores that sovereignty by manifesting it at its most spectacular. The public execution, however hasty and everyday, belongs to a whole series of great rituals in which power is eclipsed and restored (coronation, entry of the king into a conquered city, the submission of rebellious subje cts" (Foucault,1995, p. 48).

[20] Under these circumstances, political functioning had corporeal violence in a cruel ceremonial as an apparatus that reinforced the force relationship (Foucault, 1995, p. 68)

[21] From the Classical Period to Modernity, the valuation of the body changed due to the bourgeoisie ascendence, which sustained a productive logic where bodies were needed. Thus, they could longer be killed in acts of sumptuous violence, they needed to be molded in such a way that its movements were in acco rdance with the designs of the new power. Power, then, could not be an element of death, but adequacy and training.

[22] "There are no longer any of those combinations of tortures that were organized for the killing of regicides" (Foucault, 1995, p. 16)

[23] "One no longer touched the body, or at least as little as possible, and then only to reach something other than the body itself (...) the punishment-body relation is not the same as it was in the torture during public executions. The body now serves as an instrument or intermediary: if one intervenes upon it to imprison it, or to make it work, it is in order to deprive the individual of a liberty that is regarded both as a right and as property. The body, according to this penalty, is caught up in a system of constraints and privations, obligations and prohibitions. Physical pain, the pain of the body itself, is no longer the constituent element of the penalty. From being an art of unbearable sensations, punishment has become an economy of suspended rights. If it is still necessary for the law to reach and manipulate the body of the convict, it will be at a distance, in the proper way, according to strict rules, and with a much 'higher' aim. (Foucault, 1995, p. 11)

[24] This metamorphosis is intimately related with disciplinary institutions, such as prisons, hospitals, school, and a varied group of technicians, from guards, doctors, chaplains, psychiatrists, psychologists to educators, that came to replace the executioner . They define a certain political anatomy a nd power relations.

transformative period played a pivotal role in shaping modern approaches to punishment[25] and control within society. Therefore, the exercise of discipline underpins modern techniques that are responsible for power effects. Accordingly, Deleuze`s (1988) analysis of "Discipline and Punish" reaffirms the idea by stating that:

> "modern societies can be defined as 'disciplinarian'; but discipline cannot be identified with any one institution or apparatus precisely because *it is a type of power, a technology*, that traverses every kind of apparatus or institution, linking them, prolonging them, and making them converge and function in a new way" (Deleuze, 1988, p. 26, emphasis added)

Disciplinary power has as its primary function to "train" or discipline. This is a type of power that doesn't seize or take away, and the foremost function is not to simply restrict and suppress forces, as traditional notions of power might suggest, in opposition, it aims to connect and utilize them in a unified manner. Yet, it 'trains' to extract and appropriate even more effectively. Aiming to connect and utilize forces, it seeks to multiply them. So, the power is focused on shaping and molding individuals for later use. For that reason, decomposition is necessary to create singularities.

> "To sum up, it might be said that discipline creates out of the bodies it controls four types of individuality, or rather an individuality that is endowed with four characteristics: it is cellular (by the play of spatial distribution), it is organic (by the coding of activities), it is genetic (by the accumulation of time), it is combinatory (by the composition of forces). And, in doing so, it operates four great techniques: it draws up tables; it prescribes movements; it imposes exercises; lastly, in order to obtain the combination of forces, it arranges 'tactics'. Tactics, the art of constructing, with located bodies, coded activities and trained aptitudes, mechanisms in which

[25] Not of the body but the soul, which configures discipline.

> the product of the various forces is increased by their calculated combination are no doubt the highest form of disciplinary practice"[26] (Foucault, 1995, p. 167).

Contrastingly with other forms of power that treat those submissions as blocks, uniformly shaped and grouped together, disciplinary power breaks things down into smaller parts. This specific technique[27] separates, analyzes, and differentiates forces and bodies, taking them as objects and instruments of power. Advectivaly, power is recognized as "humble" and "modest"[28] that utilizes simple instruments, such as "hierarchical observation", "normalizing judgment" and "examination", which is a combination of two (Foucault, 1995).

In essence, Foucault (1995) describes a form of power that doesn't suppress individuals or forces, but rather shapes and utilizes them through careful techniques, observation, and examination. This power creates disciplined individuals, transforms larger power structures over time, and operates as a calculated and continuous practice. In addition, Foucault (1995) argues that:

> "*The exercise of discipline presupposes a device that obliges the eye to play*; an apparatus where the techniques that allow seeing induce effects of power, and where, in return, the means of coercion make clearly visible those on whom they apply. Slowly, over the course of the classical period, these "observatories" of human multiplicity are built, for which the history of sciences

[26] Foucault articulates that discipline generates four distinct types of individuality or individual traits through its control over bodies. These four characteristics are: cellular, organic, genetic, and combinatorial. Foucault highlights that four major techniques underlie these traits: constructing frameworks, prescribing maneuvers, imposing exercises, and ultimately organizing "tactics. Firstly, akin to cells, individuals are spatially placed and controlled. Just like organs within the body, specific functions, actions and behaviors are codified, thus, discipline passes through the codification of activities.In terms of genetics, it refers to the accumulation of time. Over time, discipline accumulates knowledge and information about individuals, shaping their identities and behaviors. Finally, Combinatorial characteristic pertains to the composition of forces. Discipline combines various elements, such as behaviors and actions, to create a more powerful and controlled individual.

[27] This term certifies the technological characteristic of discipline, as classified by Foucault and analyzed by Deleuze.

[28] "It is not a triumphant power, which because of its own excess can pride itself on its omnipotence; it is a modest, suspicious power, which functions as a calculated, but permanent economy. These
are humble modalities, minor procedures, as compared with the majestic rituals of sovereignty or the great apparatuses of the state" (Foucault, 1995, p.170)

> saved so little praise. Alongside the great technology of glasses, lenses, of light beams, united with the foundation of new physics and cosmology, there were the *small techniques of multiple and crisscrossed surveillances, of gazes that must see without being seen; an obscure art of light and the visible has quietly prepared a new knowledge about man, through techniques to subject him and processes to use it."* (Foucault, 1995, p.170-1, emphasis added)

The exercise of discipline presupposes the arrangement of a specific apparatus that compels visual engagement through which power can induce its effects. Concurrently with the monumental strides in optical technology[29]. Foucault brings attention to the subtle yet potent methods of discreet surveillance that permits eyes to see without being seen, prevailing the anonymity and the unverifiability of the action. Its manifestation through hierarchical observation is organized upon individuals that have an interrelationship of constant and reciprocal control, implying in a omnipresence[30]. Due to hierarchical observation, disciplinary power becomes:

> "an 'integrated' system (...) It was also organized as a multiple, automatic and anonymous power; for although surveillance rests on individuals, its functioning is that of a network of relations from top to bottom, but also to a certain extent from bottom to top and laterally, this network 'holds' the whole together and traverses it in its entirety with effects of power that derive from one another: supervisors, perpetually supervised. The power in the hierarchized surveillance of the disciplines (...) functions like a piece of machinery" (Foucault, 1995, p.177).

Disciplinary power has within its system a penal mechanism, the normalizing judgment with peculiar sanctions and instances, that does not aim to torture, but to teach, correct and

[29] In the history of science, Foucault (1995) identifies telescope, lens and light beam as part of a universe of visual technologies that serve for observation, subjection and exploitation, as mentioned in the extract of the text of the above paragraph.

[30] In this way, everyone is obliged to adapt and follow the rules, under threat of suffer micropenalties or punishments, applied according to the deviation committed and the rank hierarchical occupation within the institution.

train. The discipline is a system of a dual mechanism of gratification-punishment that evokes a sense of dual pole between good and bad that enables a classification of behavior and establishes a quantification. For instance, in this quantification game, the permanent calculation of better and worse "grades", the disciplinary scheme promotes the classification of "good" and "bad" individuals, permitting thus to define gaps, hierarchies of qualities and skill, while also punishing and rewarding. This mechanism grants a distinction between "normal" and "abnormal"[31]. In a sum, Foucault (1995) affirms that under the disciplinary power, normalizing judgment is an existing mechanism that has a function to compare, differentiate, hierarchize, classify and correct anomalies, in other words, normalizing individuals (Foucault, 1995, p. 202-209).

In the culmination of these two mechanisms lies the examination, a intertwined technique of observing hierarchy and normalizing judgment. This fusion engenders a normalizing control that affords the capacity for qualification, classification and punishment according to gathered information. It is within this collection that knowledge finds its genesis and is shaped. Examining is related to the exercise of power and the formation of certain types of knowledge. The application of these mechanisms of control by institutions stressed the accumulation of detailed information, which enabled the production of a vast material useful for knowledge formation, codification and classification. Illuminating this dynamic, Rabinow (1995/2002) writes that:

> "An extensive documentary apparatus becomes an essential part of the technologies: precise dossiers enable the authorities to fix individuals in an objective in a web of objective coding; more precise and statistically accurate individual knowledge leads to

[31] Schools are a precise example of this disciplinary conduct considering the existence of a grading system that classifies students' result according to their performance, being under a norm, as "good" or "bad". This produces a hierarchization and comparison, and gradual classification of performance that will be rewarded or punished. Those who acquire higher grades are rewarded with a promotion to higher degrees, while those who are framed as worse in this scale, are "downgraded". This dynamic recalls contemporary hierarchization mechanisms, such as China's 'social credit' system.

> more subtle and comprehensive normalization criteria" (Rabinow (1995/2002, p.46, translated by the author).

Attributed with the invisible singularity of the technique, it puts individuals in a surveillance ground that brings them to focus. In this light, Foucault (1995) underlines how the examination process effectively instills individuality into the realm of documentation:

> "The examination also introduces individuality into the field of documentation. The examination leaves behind it a whole meticulous archive constituted in terms of bodies and days. The examination that places individuals in a field of surveillance also situates them in a network of writing; it engages them in a whole mass of documents that capture and fix them. The procedures of examination were accompanied at the same time by a system of intense registration and of documentary accumulation". (Foucault, 1995, p. 213)

In the landscape of disciplinary power, Foucault's analysis brings light to an instrumental apparatus accompanied by a scheme of documentation that opens up to two correlated possibilities. Firstly, the examination facilitates the transformation of the individual into a describable and analyzable object by maintaining its singularity features. Simultaneously, the examination engenders the emergence of a comparative system, thereby affording the measurement of global phenomena, the delineation of collectives, the characterization of communal occurrences, and the quantification of deviations among individuals. This second facet embraces the statistical evaluation of disparities between individuals, their configuration within a larger "population," and the nuanced elucidation of patterns in their interrelationships. Consequently, it underpins the construction of knowledge, the exploration of power, and the composition of control mechanisms (Foucault, 1995, p. 211-216).

In this regard, power and knowledge are intrinsically related. This interdependence between these two domains implies that power not only aids knowledge but actively generates it. The reciprocal nature of power and knowledge becomes apparent, in which power operates in tandem with knowledge formation, and knowledge, in turn, serves as a vehicle for the exercise of power. This interconnection represents the concept of "power-knowledge" (Foucault, 1995, p.31).

In the contemporary era, surveillance technologies have evolved from conventional methods to highly sophisticated systems, shaping the dynamics of power and control in society. These technologies embodied some modern surveillance mechanisms aligned with principles of discrete and constant monitoring, complemented by a systematic codification. Data collection practices and the perpetual processing of information mirror the normalizing judgment mechanism, contributing to the classification and categorization of individuals based on societal norms. This synthesis captures the enduring influence of Foucault's concepts in understanding the intricate interplay between technology, power, and surveillance practices shaping the dynamics of the contemporary societal terrain. Furthermore, technical specifications become more noticeable in the next paragraphs.

Aftering having understood the role of disciplinary techniques in the exercise of disciplinary power, the panoptic technology can finally be brought to discussion once it is considered an ideal model of its exercise. As an architectural figure for this composition, it is applicable for facilities where it is necessary to keep people under surveillance[32], and therefore, it is an abstraction for the functioning of power relations. As an element to consider, it is described as known principle in which:

[32] Foucault (1995, p.229 emphasizes the high applicability of this mechanism, as a "polyvalent" application, which can be implemented in "hospitals, workshops, schools, prisons", but also considers that it might be subject to certain modifications to do so. In all cases, "whenever one is dealing with a multiplicity of individuals on whom a task or a particular form of behavior must be imposed, the panopticism schema may be used".

> "at the periphery, an annular building; at the center, a tower; this tower is pierced with wide windows that open onto the inner side o f the ring; the peripheric building is divided into cells, each of which extends the whole width of the building; they have two windows, one on the inside, corresponding to the windows of the tower; the other, on the outside, allows the light to cross the cell from one end to the other. All that is needed, then, is to place a supervisor in a central tower and to shut up in each cell a madman, a patient, a condemned man, a worker or a schoolboy. By the effect of backlighting, one can observe from the tower, standing out precisely against the light, the small captive shadows in the cells of the periphery. They are like so many cages, so many small theaters, in which each actor is alone, *perfectly individualized and constantly visible.* The panoptic mechanism organizes spatial units that *make it possible to see constantly and to recognize immediately*. (Foucault, 1995, p. 200, emphasis added).

The Panopticon, as envisioned by Jeremy Bentham, operates in permanent visibility and unverifiability that are the sustenance of power, characterized by continuity and smoothness. This dual principle firstly, entails the visual exposition of control structures, exemplified by the central tower in this case. The physical prominence of this tower functions as a constant reminder to individuals of their being under observation, fostering an awareness that even the slightest deviation from expected behavior could lead to punitive consequences. Secondly, the efficacy of this approach lies in the obscurity surrounding the watchman within the tower. In the absence of certainty about being surveilled, individuals tend to adopt a disciplined demeanor, compliant, cooperative, and self-regulate, as a means of preemptively evading any potential penalties[33]. This intricate interplay between visibility and invisibility engenders a self-regulatory mechanism within the subject (Rabinow, 1995/2002; Fleuri, 2008).

This juxtaposition of the two factors in the mechanism works to both automate and de-individualize the exertion of power, exemplifying a subtle yet potent mode of influence that serves any power apparatus (Foucault, 1995). Its performance as an intensifier scheme ensures

[33] This self-imposed restraint transforms the individual into their own custodian, as succinctly captured by Rabinow (1995/2002, p. 43, translated by the author), "if the prisoner is never sure of when he is being watched, he becomes his own guardian"

the modus operandi, the effectiveness and automation, in other words, it is an architectural idea-format that makes power relations function by enabling a deeper access to human behavioral change.

Beyond its role as a mere observatory, it is characterized as a versatile laboratory for behavior modification. As Fleuri (2008, p. 473, translated by the author) identifies, "from the other side, the observer can identify, compare and classify the behavior of individuals". It is a platform for conducting experiments, manipulating behaviors, and refining techniques of control. This extends to medical trials, disciplinary measures, and punitive methods, all tailored to the specific characteristics and infractions of individuals (Foucault, 1995). From this aspect, Foucault (1995) explores the synergy between observation and knowledge acquisition, asserting that the Panopticon's architecture enhances the efficacy of power by enabling a deeper penetration into human behavior. It is through the process of observation that power amplifies its domain, accumulating knowledge across the domains where it is carried.

In other words, Jeremy Betham's design of an architectural structure, which was previously defined, serves as the basis for the building of a generalized formula for discipline, ergo being a principle of a new political anatomy[34]. Panopticism is therefore a process of a panopticon ideal that serves as a category of analysis, a tool for understanding the basic functioning of a society completely traversed and penetrated by disciplinary mechanisms. In a sum, while the panopticon refers to the physical structure, panopticism encapsulates the broader social and psychological implications of this architectural design as it is applied across various institutions and power dynamics[35] (Foucault, 1995).

[34] "This enclosed, segmented space, observed at every point, in which the individuals are inserted in a fixed place, in which the slightest movements are supervised, in which all events are recorded, in which an uninterrupted work of writing links the centre and periphery, in which power is exercised without division, according to a continuous hierarchical figure, in which each individual is constantly located, examined and distributed among the living beings, the sick and the dead - all this constitutes a compact model of the disciplinary mechanism" (Foucault, 1995, p.197)

[35] "It is polyvalent in its application (...) Whenever one is dealing with a multiplicity of individuals on whom a task or a particular form of behaviour must be imposed, the panoptic schema may be used. It is - necessary modifications apart - applicable 'to all establishments whatsoever, in which, within a space not too large to be

In essence, Foucault's work bridges the historical past with contemporary societal constructs, offering a critical perspective on how power manifests, disseminates, and operates through a more subtle form of control. His exploration exposes the modality of discipline, characterized by uninterrupted and constant coercion, supervising processes over results, and codifying time, space, and movement, becoming a lens through which to understand contemporary surveillance techniques. Moreover, The panopticon emerges as an architectural ideal for surveillance technologies, while the Panopticism, as a category of analysis, extends beyond physical structures to encompass the broader societal implications of constant surveillance, influencing power dynamics and individual behavior in public spaces. Foucault's (1995) concept of power-knowledge becomes particularly relevant in understanding how surveillance not only controls but actively generates knowledge about individuals and populations, providing a theoretical framework for comprehending the current situation on surveillance techniques in the public security sector.

1.2 Decoding the landscape of surveillance studies

In the contemporary landscape, the ubiquity of surveillance technologies has extended their systematic monitoring across various facets of society, spanning communication, work, leisure, and consumption. This widespread surveillance practice entails the routine collection

covered or commanded by buildings, a number of persons are meant to be kept under inspection'" (Foucault, 1995, p.205-6).
For instance, the police institution serves as a quintessential manifestation of panopticism in modern society. The relationship between the police and panopticism can be understood as an example of how discipline manifests itself in a given institutional context. Just like Bentham's panopticon, in which a central observer has the power to surveil all prisoners without being seen, the police exercise constant control over society through specific techniques and procedures. The police act as an instrument of disciplinary power, ensuring conformity and social order through surveillance and protection. In this sense, it is one of the mechanisms used by the State to exercise control and power over individuals, reinforcing an existing power structure. The police, like other disciplinary institutions, seek to standardize behavior and eliminate any form of deviation from the established norm. In short, the relationship between the police and panopticism shows how the discipline becomes a technology of power, present in different institutions and social apparatuses.

of data, serving diverse purposes such as descriptive analysis and pattern identification. Given the technological advancements and building upon the concepts previously discussed, it is crucial to examine the contextual role of surveillance systems in the realm of public security studies. To address this, the methodology for this section relies on a thorough literature review, engaging with insights from contemporary scholars deeply entrenched in ongoing studies on surveillance.

The continued relevance of Foucault's concepts urges us to engage in profound reflections on the contemporary mechanisms of control, underscoring the lasting significance of his ideas in understanding the complexities of the world.

In pursuit of this objective, Michel Foucault's influential work "Discipline and Punish" (1995) will be drawn upon through a strategic curation of relevant concepts, precisely tailored to align with the scope of this study. The exploration of disciplinary mechanisms, deeply rooted in historical contexts, exhibits a remarkable resonance with contemporary advancements in the realms of surveillance technologies. Parallels between the classical observatories and contemporary surveillance systems can be revealed. Foucault's insights illuminate this connection, as his work exposes under discipline scope, means and methods of control that are interlinked with documentation and examination techniques.

In this manner, the act of close examination that positions individuals within the realm of surveillance also positions them within a network of written records. This process involves an extensive collection of documents that not only capture their details but also establish them in a definitive manner. It is placed within a system of "intense registration and of documentary accumulation"[36] (Foucault, 1995, p.189). As "means of control and method of domination", description becomes a document for "eventual use" and no longer belongs to the mere act of

[36] As already highlighted, "the examination that places individuals in a field of surveillance also situates them in a network of writing; it engages them in a whole mass of documents that capture and fix them. The procedures of examination were accompanied at the same time by a system of intense registration and of documentary accumulation" (Foucault, 1995, p.189).

preserving their legacies for posterity, serving consequently to a process of objectification and subjection[37] (Foucault, 1995, p. 216; Matzner, 2017).

> "The examination leaves behind it a whole meticulous archive constituted in terms of bodies and days. The examination that places individuals in a field of surveillance also situates them in a network of writing; it engages them in a whole mass of documents that capture and fix them. The procedures of examination were accompanied at the same time by a system of intense registration and of documentary accumulation. A 'power of writing' was constituted as an essential part in the mechanisms of discipline. (...) On many points, it was modelled on the traditional methods of administrative documentation, though with particular techniques and important innovations. Some concerned methods of identification, signalling or description"[38] (Foucault, 1995, p.189)

On discussion on surveillance and the use of data, Foucault's insights not only illuminate historical developments but also stimulate critical inquiries into the intricate interplay between visibility, power, and technological progress. The uninterrupted nature of the examination mechanism engenders significant implications for the collection of data. Beyond the process confined to production and storage, examination persists as an ongoing endeavor characterized by constant updates. This perpetual evolution generates consequential outcomes for the subjects under scrutiny, within the framework of power. This process is substantiated by a continuous operation of cumulative documentation, marked by seriation,

[37] "Disciplinary procedures have revised this relationship (...) No longer a monument for future memory, but a document for eventual use. And this new describability is all the more marked because the disciplinary framework is strict: the child, the sick person, the madman, the convict will become, more and more easily from the 18th century onwards and in accordance with the mechanisms of discipline, the object of individual descriptions and biographical accounts. This written transcription of real lives is no longer a process of heroification; it functions as a process of objectification and subjection. The carefully studied lives of the mentally ill or delinquents originate, like the chronicle of kings or the epic of the great popular bandits, from a certain political function of writing, but in a totally different technique of power. (Foucault, 1995, p. 192, emphasis added)

[38] Similar to the current technological capacity, Foucault (1995, p.189) writes "The register enables one, by being available in time and place, to know the habits of the children, their progress in piety, in catechism, in the letters, during the time they have been at the School' (M.I.D.B., C4)."

meticulous organization, and the deployment of comparative tools. These mechanisms collectively facilitate the classification and hierarchical arrangement of subjects, enabling comparisons, the establishment of categorical distinctions, and the formulation of norms.

> “Thanks to the whole apparatus of writing that accompanied it, the examination opened up two correlative possibilities: firstly, the constitution of the individual as a describable, analysable object, not in order to reduce him to 'specific' features, as did the naturalists in relation to living beings, but in order to maintain him in his individual features, in his particular evolution, in his own aptitudes or abilities, under the gaze of a permanent corpus of knowledge and, secondly, the constitution of a comparative system that made possible the measurement of overall phenomena, the description of groups, the characterization of collective facts, the calculation of the gaps between individuals, their distribution in a given 'population'.”[39] (Foucault, 1995, p. 190)

Incorporating this conceptual framework, it is possible to discern contemporary landscape in terms of data-collection, process and knowledge production. In light of these developments, Matzner (2017) perceives information technology as a catalyst for rapid data storage and transmission, coinciding with the widespread integration of sensors and mobile devices, resulting in an extensive reservoir of accessible data. Consequently, the generation, manipulation, and interpretation of data, along with subsequent decision-making processes, is still linked to a demand for ever more data that is always actualized.

The contemporary conditions of data collection, processing, and knowledge production aligns with the characteristics of repetition and regularity. As affirmed by De Laat (2019), pre-existing data collection practices were already in place prior to the advent of the Big Data era. These practices involved institutional entities engaged in the systematic accumulation of data. However, the contemporary scenario reveals a transformation wherein supplementary datasets

[39] Notably, this process can be critically related to China’s social credit system, for example.

are now acquired externally, drawing from diverse sources. Furthermore, these collected datasets are subject to consistent interchange between institutions, which will be later discussed.

Within the framework of disciplinary logic, the consistent observation and documentation of information were integral aspects. Data obtained from disciplinary institutions regarding individuals effectively transformed into instruments for political control. The continual surveillance facilitated the ongoing refinement of information, serving as a basis for thorough analysis. Established routines were cemented, disciplinary boundaries were enforced, and standardized norms were applied in an attempt to homogenize individual behavior.

> "In a sense, the power of normalization imposes homogeneity; but it individualizes by making it possible to measure gaps, to determine levels, to fix specialities and to render the differences useful by finding them one to another. It is easy to understand how the power of the norm functions within a system of formal equality, since within a homogeneity that is the rule, the norm introduces, as a useful imperative and as a result of measurement, all the shading of individual differences." (Foucault, 1995, p.184)

Starting from the centrality of observation and surveillance, it becomes evident that within the disciplinary paradigm, the process of observing and recording information followed a systematic and consistent pattern. Information about individuals, gathered from disciplinary institutions, metamorphosed into potent tools for political control. The continual surveillance facilitated the constant updating of information, which was employed for scrutinizing subjects. Routines were rigidly fixed, disciplinary spaces tightly regulated, and imposed norms were unchanging.

Bringing it to the current context, De Laat (2019) offers insight into the convergence of Foucauldian discipline and the surveillance landscape and its related power mechanisms. Under the Foucaudian paradigm, discipline as a form of governance involved the observation, analysis, and examination of individuals. Those who were deemed abnormal in relation to prevailing norms were subjected to disciplinary measures. The aim was to mold individuals into docile bodies by compelling conformity with established institutional norms.

Consequently, the apparatuses of the disciplinary writing produces data, store, create and analyze it, which allows the creation of individuals and perceive them within the population. In this case, disciplinary techniques follow the existing norms, making an effort to make individuals act according to that. In this context, the term "normatization" assumes significance, denoting the presence of pre-established norms that individuals were expected to adhere to. Compliance with these norms was rigorously monitored and enforced through disciplinary techniques[40] (Matzner, 2017; De Laat, 2019).

The concept of "normation" within this paradigm revolves around evaluating an individual's adherence to established norms. In the traditional Foucauldian paradigm, it is prioritized the identification and punishment of concrete deviations or criminal actions, focusing on the offense itself. De Laat's (2019) central proposition involves a nuanced interpretation of the traditional paradigm, identifying an additional mechanism which extends a normation already in existence. De Laat (2019) develops a classification as follows:

> “Primary discipline is put into action as soon as a subject breaks—or appears to be about to break—the norm; the secondary mechanism of discipline based on prediction (...) may suggest an intervention even before that: as soon as a subject appears likely to be breaking a norm sometime in the future. The former discipline had to wait until norm deviance happens or seems

[40] De Laat (2019) writes that “In Discipline and Punish this process of normation has the following meaning. All subjects involved are drawn into a comparative field which, by its very existence, exerts a pressure to conform.”

> immanent; the latter anticipates it and acts accordingly. In the case of burglary: wait until the break-in actually happens, or appears to be about to happen (primary discipline), or in anticipation put the suspect under close surveillance (secondary discipline)." [41](De Laat, 2019, p.323)

In the traditional Foucauldian discipline, intervention occurred primarily when a subject deviated from or appeared to be on the verge of breaking a norm, essentially, a form of primary discipline. Hence, De Laat (2019) proposes a nuanced and anticipatory dimension to disciplinary power with a significant departure from the act to the potential offender. It intervenes not only when deviance is imminent but also when there's a likelihood of norm violation sometime in the future. In a sum, predictive modeling introduces secondary discipline, which anticipates norm violation.

Building upon this conceptual framework, it is imperative to go deeper into the nuanced implications of disciplinary mechanisms that shape behaviors and foster conformity. In the contemporary landscape, marked by the omnipresence of technologies like facial recognition, biometric tracking, and data analysis, the consciousness of constant surveillance serves as a reflection of the internalized control intrinsic to disciplinary power. This heightened awareness of being under constant observation not only highlights the evolving dynamics of discipline but also emphasizes the interplay between technology, institutions, and the individuals they govern.

[41] In a sequential fashion, Matzner (2017, p.38) revisits and reevaluates the notions of normalization and normation, ultimately asserting that these processes consolidate into a hybrid form. This hybrid form, as elucidated by Matzner, involves both normation practices and normalization techniques. Once the concept of normation was above explained, it is now possible to consider the understanding of normalization. Within this framework, as posited by Matzner (2017), norms are constructed through the process of data mining and pattern identification. Consequently, individuals labeled as deviating from these constructed norms become subjects of control, contributing to the formation and reinforcement of these norms. In this context, Matzner (2017) reveals a nuanced interplay between norms and data mining. Norms are dynamically constructed through data analysis and pattern recognition. Individuals perceived as deviating from these evolving norms become subjects of control, contributing to the ongoing shaping and redefinition of societal norms.

Moreover, in the light of the data-based surveillance discussion, Matzner (2017) investigates the outcomes of mechanisms involved in the data acquisition, processing and carried-out actions based on that. He perceives an increase in data availability that no longer belongs to enclosed intuitions, which characterizes a distributive behavior. Based on that assessment, Matzner (2017) notices a complementary feature with Foucault, especially in terms of policing. Although he recognizes a disciplinary mechanism, he emphasizes the non-localized and widespread surveillance. In the present, the generated data finds its place within interconnected datasets, facilitating the integration of various spheres of life. This evolution has expanded the realm of surveillance from confinement spaces to encompass data sourced from diverse sectors and contexts, thereby creating a concept akin to "super-surveillance" (De Laat, 2019).

De Laat (2019, p.323) provocatively raises the question: "Can this be interpreted using the metaphor of the Panopticon?" His response leans towards affirmation, albeit in a dual sense. Firstly, from the standpoint of the "focal" institution, individuals are compelled to assume the continuous generation and collection of pertinent data, a manifestation of routine Panopticism. Secondly, individuals must also recognize their entanglement within various digital "Panoptica," where other traces about them are continually monitored and archived. Subsequently, these assorted data sets can be retroactively incorporated into the focal institution under consideration, significantly enhancing machine learning endeavors, often yielding unforeseen insights. This confluence of panoptic gazes across disparate contexts can be termed a "polypanopticon." This term encapsulates the paradigm shift where individuals, formerly subject to concealed surveillance within closed disciplinary spaces[42], now exist within a regime of pervasive and unrestrained surveillance.

[42] "This enclosed, segmented space, observed at every point, in which the individuals are inserted in a fixed place, in which the slightest movements are supervised, in which all events are recorded, in which an uninterrupted work of writing links the centre and periphery, in which power is exercised without division, according to a continuous hierarchical figure, in which each individual is constantly located, examined and distributed among the living

As a result, and due to the enormous volume of data available, discipline would have occurred in a heterogeneous and spaced-out manner. Notably, some scholars in surveillance studies emphasize that contemporary surveillance practices have transcended the confines of closed institutions[43]. Complementary, for instance, to Matzner's (2017) perception that data have become independent of the spatial configuration of closed institutions, Shoshanna Zuboff (2015, p.82) writes:

> "These processes reconfigure the structure of power, conformity, and resistance inherited from mass society and symbolized for over half a century as Big Brother. Power can no longer be summarized by that totalitarian symbol of centralized command and control. Even the panopticon of Bentham's design, which I used as a central metaphor in my earlier work (Zuboff, 1988, Ch. 9,10), is prosaic compared to this new architecture. The panopticon was a physical design that privileged a single point of observation. The anticipatory conformity it induced required the cunning production of specific behaviors while one was inside the panopticon, but that behavior could be set aside once one exited that physical place".

The production of data and the subsequent actions drawn from it transpire across varying temporal and spatial dimensions. Consequently, data has transcended its reliance on the architectural structure of isolated institutions[44].

The interpretation of the term "Panopticon" and its applicability to current surveillance mode has guided differing opinions among scholars. Some advocate for its transformation[45], while others suggest its abandonment. In the latter, Kevin D. Haggerty (2006) adopts a more extreme stance, asserting that contemporary shifts in surveillance processes and practices

beings, the sick and the dead - all this constitutes a compact model of the disciplinary mechanism" (Foucualt, 1995, p.197)

[43] For instance, Matzner (2017, p.33) concludes that "data thus have long become independent of the spatial configuration of closed institutions."

[44] This perspective is aligned with the Deleuzian perspective expounded upon in "Postscript for the Societies of Control" (2006).

[45] In "Tear down the walls: on demolishing the panopticon", Kevin D. Haggerty (2006, p. 26) presents the existence of many other 'opticon' description that somehow follows Foucaudian perspective, he writes: "In addition to the superpanopticon, electronic panopticon and postpanopticon, there are references to the 'omnicon' (Goombridge 2003), 'ban-opticon' (Bigo this volume), 'global panopticon' (Gill 1995), 'panspectron' (De Landa 1991), 'myoptic panopticon' (Leman-Langois 2003), 'fractal panopticon' (De Angelis 2001), 'industrial panopticon' (Butchart 1996), 'urban panopticon' (Koskela 2003), 'pedagopticon' (Sweeny 2004), 'polyopticon' (Allen 1994), 'synopticon' (Mathiesen 1997), 'panoptic discourse' (Berdayes 2002), 'social panopticism' (Wacquant 2001), 'cybernetic panopticon' (Bousquet 1998), and the 'neo-panopticon' (Mann, Nolan and Wellman 2003)".

erodes the relevance of the panoptic model[46], and besides the architectural structure difference, he reveals a broader purpose of surveillance that extends beyond mere social control[47]. This perspective highlights a fundamental departure from the traditional Panopticon framework, signaling the need to reevaluate the understanding of surveillance in light of its multifaceted contemporary manifestations. Less assertively on the denial of Foucault's approach to surveillance, Matzner (2017) considers some of Foucault's analysis' elements are still applicable to today's information society at some level [48].

It is important to perceive the panoptic arrangement as a replicable mechanism, or in Foucault's words (1995, p. 209) a "formula" that enables generalization and penetration into other functionalities of society through a disciplinary mechanism, which concept is explained in the previous section. In fact, the previous extension of a singular format to a replication of a logic into other modern institutions[49] permits a critical consideration of panopticism beyond a limited locality, infiltrating into contemporary arrangements. Echoing the sentiment expressed by De Laat (2019, p.328), it is observed that, "it has been demonstrated that tools from the Foucauldian toolkit remain valuable for dissecting contemporary surveillance practices."

After delineating this divergent standpoint, it becomes pertinent to acknowledge that Michel Foucault conducted his research during the latter half of the 20th century, affording a

[46] "Foucault continues to reign supreme in surveillance studies and it is perhaps time to cut off the head of the king. The panoptic model masks as much as it reveals, foregrounding processes which are of decreasing relevance" (Haggerty , 2006, p.23). In the same book David Lyon (2006, p. 12) writes that "Haggerty makes no bones about his project: 'Tear down the walls'! He comments effectively on 'demolishing the panopticon', a project that has several significant rationales. His key point is that what might be called panopticism as an all-embracing model or paradigm should be abandoned".

[47] "This proliferation of surveillance has also meant that more and more people at home, work or leisure are constituted as viewers. Such surveillance is not just a function of rationalizing regulatory projects, but can also be enjoyable. Both watching others and exposing oneself can, at times, be pleasant entertainment activities, and are themselves occasionally part of larger processes of identify formation." By this statement, it is possible to affirm that Kevin D. Haggerty challenges the notion that it is always undesirable or invasive. They highlight the potential for positive experiences and argue that surveillance can be a source of pleasure. By presenting this perspective, the author fosters a more liberal and accepting attitude towards the increasingly pervasive presence of surveillance in everyday life.

[48] Still, according to Matzner (2017), disciplinary society would no longer be sufficient to describe and analyze power relations in the information society, while Deleuze's writings, in his Post Scriptum (1992), would better translate the new sociopolitical configuration.

[49] Schools, military, hospital, etc.

historical remove from his subjects of investigation, which pertained to the 17th and 18th centuries. Conversely, the current study is developed within the very technical and social milieu shaped by the subject under scrutiny, the 21st-century surveillance dynamics. As a result, the intention was not to contemporize Foucault's ideas by reinterpreting his writings through novel lenses or formulating fresh 'truths' derived from them. Instead, the aim was to operationalize select concepts primarily from “Discipline and Punish”, channeling them into a critical analysis of the contemporary landscape of technopolitical surveillance.

In conclusion, this chapter has undertaken a comprehensive exploration of the interplay between surveillance, power, and technology, drawing from the seminal works of Michel Foucault and insights from contemporary surveillance scholars. Overall, the analyses and examinations conducted in the sections “Exploring Michel Foucault's Theoretical Framework on Surveillance” and “Decoding the Landscape of Surveillance Studies” underscores the dense and multifaceted nature of contemporary surveillance practices. These ideas shed light on the dynamics of power, control, and compliance in an era characterized by pervasive technological surveillance, highlighting the need for continued critical analysis in the field of surveillance studies.

Moving forward, the next chapter will delve into the practical applications of surveillance technologies within the public security sector. It will examine how these technologies are shaping the scope of public security, especially in Brazil, raising important ethical and legal questions that demand thoughtful consideration and discussion.

CHAPTER 2

The use of surveillance in public security sector

In the digital age, the proliferation of interconnected devices, applications, and cameras has ushered in a new era of surveillance practices. These practices have evolved with technological advancements, enabling novel methods of measurement, tracking, and the surveillance of individuals, along with the control of their behaviors. Hence, surveillance became a feature of today's technologies and an infrastructure of devices and systems ranging from applications to data processing software biometrics. Due to its omnipresence, it is substantial to understand the complexity of those practices by exploring the multiplicity of applications and purposes.

To effectively comprehend the ramifications of this technology, it is paramount to initially discern where these tools are being deployed and the manner in which they are utilized. The primary objective of this section is to elucidate how emerging surveillance capabilities are reshaping governments' capacity to monitor and trace individuals or systems. This section will delve into various instances of surveillance technology implementation within the realm of the security sector.

Amid apprehensions surrounding “dystopian” projects, such as China's social scoring system, and concerns regarding the misuse of these technologies by authoritarian regimes, there exists a spectrum of possibilities for the application of surveillance-based systems (Instituto Igarapé, 2022, p.2). Surveillance technology is currently in use in at least 75 out of 176 countries for surveillance purposes (Feldstein, 2019). Rather than polarizing discussions to the extremes, this study aims to strike a middle ground by examining a case of surveillance, focusing on the Global South. This region serves as a crucible for testing emerging trends and widespread deployment of such technologies, often in contexts that lack the technical infrastructure and legal frameworks to effectively regulate them (Instituto Igarapé, 2022).

2.1 Brazil's security context and the application of surveillance technologies

The expansion of interconnectivity and the evolution of information and communication technologies has given rise to innovative mechanisms towards crime prevention and suppression. In this dynamic context, technology emerges not only as a tool for law enforcement but as a catalyst shaping the contours of public security policies.

In the context of this research, Brazil assumes a significant position within the broader global context. Its relevance emanates from factors including its geographical expanse and its substantial population[50], which can significantly contribute to data generation. Moreover, Brazil has embraced surveillance technology, manifesting in various forms, including its utilization in smart city and safe city platforms, the deployment of facial recognition systems, and its integration into smart policing initiatives (Feldstein, 2019; AIGS, 2022). In general, 237 cases of the employment of surveillance technologies were monitored from 2006 to 2022 by the Instituto Igarapé (2022), according to their report entitled "Implantação de Tecnologias de Vigilância no Brasil e na América Latina".

As Brazil navigates the dynamic terrain of contemporary security challenges, the interplay between constitutional principles and technological advancements in surveillance becomes increasingly significant. The constitutional provisions establish the framework for law enforcement agencies but also offer a legal basis for adapting to emerging security

[50] See the annexes containing information about the Brazilian population and its distribution within the territory, as well as the map indicating states and regions.

paradigms. Within this intricate interplay of societal evolution and technological influence, Article 144 of the Brazilian Constitution emerges as a foundational for this discussion:

> Art. 144: Public security, the duty of the State, the right and responsibility of all, shall be exercised for the preservation of public order and the safety of persons and property, through the following bodies: I - federal police; II - federal highway police; III - federal railroad police; IV - civil police; V - military police and military fire departments. § Paragraph 1 The federal police, established by law as a permanent body, organized and maintained by the Union and structured into a career, is intended to: (Edited by EC 19/1998). § Paragraph 2 The federal highway police, a permanent body, organized and maintained by the Union and structured into a career, is intended, in accordance with the law, for the ostentatious patrolling of federal highways. (Edited by EC No. 19/1998). § Paragraph 3 The federal railroad police, a permanent body, organized and maintained by the Union and structured into a career, is intended, in accordance with the law, for the ostentatious patrolling of federal railroads. (Redacted by EC 19/1998). § Paragraph 4 - The civil police, headed by career police chiefs, shall be responsible, with the exception of the Union's powers, for the judicial police and the investigation of criminal offenses, except for military offenses.§ Paragraph 5 - The military police shall be responsible for ostensible policing and the preservation of public order; the military fire departments, in addition to the duties defined by law, shall be responsible for carrying out civil defense activities. § Paragraph 6 - The military police and military fire departments, auxiliary and reserve forces of the Army, shall be subordinate, together with the civil police, to the Governors of the States, the Federal District and the Territories. § Paragraph 7 - The law shall regulate the organization and functioning of the bodies responsible for public security, in order to guarantee the efficiency of their activities. § Paragraph 8 - Municipalities may set up municipal guards to protect their goods, services and facilities, in accordance with the law. § Paragraph 9 - The remuneration of police officers who are members of the bodies listed in this article shall be set in accordance with Paragraph 4 of Article 39. (Included by EC 19/1998) § 10 Road safety, exercised for the preservation of public order and the safety of people and their property on public roads: (Included by EC 82/2014). (Brazilian Federal Constitution, 1988).

In a sum, Article 144 of the Brazilian Federal Constitution (1988) lays the foundation for the nation's approach to public security, emphasizing it as a duty of the State, a right, and a responsibility for all citizens. Besides, it delineates the entities responsible for ensuring security, among them are the Federal Police, Civil Police, and the Military Police (Constituição Da República Federativa Do Brasil, 1988).

After the indispensable presentation of public security in the legal framework prescribed by the Brazilian Federal Constitution, it is possible to unfold the relationship with the progressive integration of surveillance technologies. This integration, shaped by the principles of prevention, justice, and societal reintegration, paints a nuanced picture of Brazil's endeavor to balance security imperatives.

In response, the Brazilian Federal Government launched the 2021-2030 National Public Security Development Plan (PNSP). Outlined in Article 6 of Law No. 13.675 (Lei 13.675, 2018), there exists a distinct focus on promoting measures that propel the modernization of equipment, investigation along with standardizing the technology across security entities. Specifically, Strategic Action 7 envisions a future where technology plays a pivotal role in the standardization, integration, and interoperability of security-related data at various governmental levels[51]. This initiative envisions an innovative approach to the application of cutting-edge tools in public security, aligning the Union, States, Federal District, and Municipalities, with the foremost aim of enhancing the efficiency and efficacy of national public security efforts (Plano Nacional de Segurança Pública e Defesa Social 2021-2030, 2021).

[51] Strategic Action 7: Technologically standardize and integrate public security databases between the Union, States, Federal District and Municipalities through the implementation of the National Public Security, Prisons, Weapons and Ammunition Traceability, Genetic Material, and Drugs - Sinesp and the National Penitentiary Department Information System - Sisdepen and through data obtained from the National Traffic System - SNT and other systems of interest to public security and social defense, using machine learning tools for categorization and analysis. (Plano Nacional de Segurança Pública e Defesa Social 2021-2030, 2021, translated by the author).

The utilization of surveillance technologies is not a recent phenomenon but rather part of a continuous and escalating process. This evolution can be traced back to significant events such as international sporting events like the World Cup, urban development plans geared towards the establishment of smart cities, or responses to crises related to urban and public health security[52] (Instituto Igarapé, 2022). To address those issues, the deployment of these technologies is often justified, incurring in a techno-solutionism tendency[53]. Building upon the evolution of surveillance technologies earlier discussed, it is evident that Brazil's enthusiasm for solutionism is influenced by present vulnerabilities in the public security sector.

To put this into perspective, Brazil holds the distinction of having the highest absolute number of homicides globally and ranks as the eighth most violent country in the world, according to the United Nations Office on Drugs and Crime (UNODC) (Fórum Brasileiro de Segurança Pública, 2022). Despite comprising only 2.7% of the world's population, Brazil accounted for a staggering 20.4% of the 232,676 homicides reported in 102 countries in 2020 (Fórum Brasileiro de Segurança Pública, 2022). This stark reality underscores the gravity of the security challenges facing the nation.

[52] Naomi Klein presents the idea of a ‘shock doctrine’, which is a philosophy of power that imposes ideas subsequent to a major shock which can range from economic, natural, human catastrophe such as wars and terrorist attacks. In this sense, it can be said that the COVID-19 health crisis can be seen as a window of opportunity for the more incisive introduction of a logic of power which is linked to new technologies. For further discussion, see: Salvo, Philip Di. Solutionism, Surveillance, Borders and Infrastructures in the “Datafied Pandemic”. In COVID-19 from the Margins: Pandemic invisibilities, Policies and Resistance in the Datafied Society. Milan, S.;Treré, E.; Masiero, S. (edit). Theory on Demand #40. Amsterdam, Institute of Network Cultures, 2021 pp. 164 - 170; and Lyon, D. (2021). Pandemic Surveillance. John Wiley & Sons.

[53] Instituto Igarapé (2022) reports the implementation of surveillance technologies in Brazil has followed a trend since 2006, with notable peaks in 2010, 2013, 2018, and 2020. The first peak in 2010 might have been triggered by a major security crisis in Rio de Janeiro, leading to a government intervention and the occupation of favelas by local police forces, the Brazilian Army, and Marine Corps. The second peak in 2013 can be attributed to both social movements against the government and the hosting of the World Cup, which likely influenced the expansion of surveillance measures. The third peak in 2018 occurred due to a Federal intervention in Rio de Janeiro. Finally, the COVID-19 pandemic in 2020 might have served as an influential factor for the implementation of surveillance tools, given the need for monitoring and controlling the spread of the virus. it is crucial to recognize that these endeavors do not exist in isolation; once these technologies are intricately woven into the existing infrastructure, it is also intersectoral. Instituto Igarapé (2022) reported the existence of facial recognition intelligence in Brazil back in 2011, although for the transport sector.

Furthermore, when analyzing the intentional violent death rates per 100,000 inhabitants, Brazil ranks as the eighth most violent country in the world based on 2020 data provided to UNODC, with a rate of 22.45 homicides per 100,000 people (Fórum Brasileiro de Segurança Pública, 2022). Within this disconcerting context, Brazil is home to 10 of the 50 most dangerous cities globally. Beyond the sheer volume of homicides, the homicidal violence is assessed in relative terms, considering the population of each country. Brazil's rate is nearly three times higher than the threshold considered epidemic by the United Nations Development Programme (UNDP), which is 10 deaths per 100,000 inhabitants[54] (UNDP, 2021).

In the Global Peace Report of 2022, Brazil receives a low-security rating, reflecting its challenging security environment (Institute for Economics and Peace, 2022). Furthermore, it ranks among the countries with the lowest scores in the "Societal Safety and Security domain" (Institute for Economics and Peace, 2022, p. 93), emphasizing the pressing need for innovative solutions to address the complicated security issues the country faces. This context underscores the motivation behind Brazil's fervent embrace of surveillance technologies as part of its multifaceted approach to enhancing public security and safety[55].

In view of these circumstances, marked by a myriad of challenges, Instituto Igarapé's Report (2022) identifies a concentration of projects implementing surveillance technologies in public security sector, representing 76% of the cases in Brazil[56].

[54] "Brazil recorded 30 homicides per 100,000 people" according to the report of Independent Country Programme Evaluation of UNDP.

[55] Additionally, the global sanitary crisis of COVID-19 that persisted for a couple of years was an intensifier factor for the adoption of innovative technologies under the governmental scope towards social tracking, information provision requests and data management. These and other challenges were significant for the employment of surveillance technologies based on artificial intelligence (AI) as solutions for sectors such as health, public safety, border control, transport and between others.

[56] The report provides a crucial methodology to elucidate the utilization of surveillance technology across various sectors and specific applications. These sectors encompass economy, education, events and tourism, intelligence, health, public security, and transports. The initial graph within the report offers a comprehensive overview of the adoption of surveillance technology by each sector. Notably, the public security sector leads with 181 instances, followed by the health sector in second place with 35 cases of implementations.

For further enlightenment, the public security sector comprises not only law enforcement agencies such as the police and military forces but also various entities within the broader criminal justice system. In this intricate web of security concerns, a multifaceted role is assumed, primarily geared towards enhancing control mechanisms and supporting preventive measures[57]. For instance, De Laat (2019) also acknowledges this aspect as a predictive modeling technique utilized by various local authorities[58] to address a wide range of social factors, such as criminality[59]. By analyzing historical data and patterns, these technologies can identify potential areas prone to criminal activity, facilitating law enforcement agencies in resources deployment.

In the existing literature, there is recognition that many surveillance technologies significantly boost the operational capabilities and coercive power of security forces. This augmentation, however, leads to the emergence of vigilantism in strategies employed for combating crime. The adoption of surveillance technologies influences this trend by introducing novel perspectives on remote policing, categorization, and group control, all intertwined with the evaluation of risk levels[60] (Feldstein, 2019). In essence, the increased technological prowess of security forces, facilitated by surveillance technologies, can foster a shift towards more proactive and potentially controversial methods of maintaining public order and addressing criminal activities.

The utilization of surveillance technologies and related tools within the public security sector signifies a strategic response to the dynamics of contemporary security threats. These

[57] See the theoretical discussion on those topics within the context of the digital era in the above sections.

[58] This demonstrates the adoption by classical institutions, as described by Foucault.

[59] De Laat (2019, p.322) write that "Local authorities, for their part, have more recently initiated innovative prediction efforts in order to curb youth crime, child abuse and domestic violence, and fraud with social security benefits or local taxes. Finally, we must not forget the classical sectors as analyzed by Foucault (some public, some private): prisons, the army, schools, hospitals, and factories. Recently, predictive modeling has been gaining a foothold in those sectors as well."

[60] As described by Steven Feldstein (2019), AI surveillance is not an independent means of oppression. It is one of several digital tools utilized for repressive purposes, including monitoring, intimidating, manipulating, and troubling adversaries with the aim of punishing and preventing any actions or beliefs that challenge the government.

technologies empower[61] law enforcement agencies and related bodies with improved monitoring capacity and complex data streams that give insights into criminal activities and potential threats.

The evolution of surveillance technologies in Brazil is driven by a context marked by vulnerabilities in the public security sector, such as the presented rates of intentional violent death. It is rooted in constitutional assessment that establishes the foundation for public security, and complemented by policies that indicate an imperative need for innovative solutions. Embracing surveillance technologies, as evidenced by 76% of projects concentrated in the public security sector, reflects a proactive stance in addressing these challenges.

Finally, in order to better understand the technological employment of surveillance tools of analysis and monitoring by public security institutions, it is necessary to describe key surveillance techniques and how the government is applying them to support specific security objectives.

2.2 Mapping the national security panorama on the use of surveillance technologies

In an increasingly interconnected and digital world, the intersection of technology and security has become a critical focal point for nations worldwide. In Brazil, there has been a noticeable emergence of a dynamic and progressing domain with the integration of technology within the security sector. Taking into consideration the above exposed background that underpins the security panorama, it is necessary to map the current state of technology use, tools and techniques, by the key stakeholders in the sector, including law enforcement agencies, military forces.

[61] This term is here allocated in order to express an alignment of the practices with Focault's power-knowledge relationship theory.

The effort to map out the use of surveillance technologies within the national panorama begins with the extensive collection of documents, including news articles, reports, academic papers, and official publications. It was opted to start by the classification and categorization of technologies in order to outline the bigger picture and understand, based on that, the use of such technologies by Brazilian security agencies. Accordingly, the main technologies are: facial recognition, bodycams, drones, and optical character recognition[62] (FGV Direito Rio, 2023; Instituto Igarapé, 2022).

Steven Feldstein (2019) characterizes facial recognition as a biometric technology system employing cameras, either through still images or video footage, to facilitate identity verification via data collection and analysis. This detection process hinges on the application of artificial intelligence for automation, primarily involving the processing of facial data. Initially, upon capturing an individual's facial image, the system proceeds to pinpoint specific facial metrics, such as interocular distance, chin width, and mouth length. Utilizing these parameters, the software computes a unique facial signature, which serves as the foundational identifier for the individual[63] (Reis et.al, 2021).

Facial recognition technology is being utilized by various security forces across Brazil, being present in all States of the country, presenting at least 195 projects regarding this technology (Mello, 2023). Notable states at the forefront of adopting this technology include Acre, Amazonas, Roraima, Pará, Bahia, Minas Gerais, Goiás, Espírito Santo, and Paraná.

In the Northern Region, it is possible to highlight the programme entitled "Rio Branco Mais Segura", which in English can be translated as "Safer Rio Branco", launched in February 2022, focuses on the installation of more than 300 video surveillance cameras throughout the

[62] It is important to note that in all consulted bibliography the definitions and classifications of each technology is not perfectly clear and usually overlapping.

[63] Anticipating the discussion, the use of facial recognition is controversial considering the racial and gender bias, which influences those groups.

city[64] (Verus, 2022). This equipment is in addition to the more than one hundred cameras and other devices at the Integrated Command and Control Center, the department responsible for video monitoring (Verus, 2022). The justification for the implementation of this project lays on the aim to reduce criminality and to enhance safety. The project places the municipality in the concept of a smart city, and the cameras have been installed at strategic points in the capital, including squares, parks, streets and bus terminals (Verus, 2022).

In Amazonas, facial recognition technology was applied in surveillance cameras for urban landscape, and the analysis of Fundação Getúlio Vargas (2022) identified more than 40 in the capital, Manaus, provided by Motorola through a bidding process. Another initiative that must be highlighted is technology which allows the facial recognition of fugitives from justice and the identification of license plates of vehicles with theft or robbery restrictions[65]. In this case, the application was developed by the Operational Command of the Military Police of Amazonas[66] (Secretaria de Segurança Pública do Estado do Amazonas, 2020).

Moreover, in 2023, the State Government, through the Secretariat for Penitentiary Administration (SEAP), has acquired monitoring equipment to improve and expand the Security Camera Monitoring System, which will be installed at the administrative headquarters and in the capital's prison units[67], among the equipment are pieces of software designed to record, display, retrieve and send alerts; cameras, and cameras with motion detection, and with facial recognition[68] (SESP, 2023).

[64] According to the head of the City Hall's Department of Modernization, Information and Communication, there are 200 fixed cameras, 50 360-degree Speed Domes cameras and 36 cameras with license plate reading, in addition to 15 cameras with facial recognition.

[65] The official webpage states that “with artificial intelligence, the military police officers can recognize the offending citizen using the camera on their cell phone. They can find out if the individual already has an open arrest warrant and, at the same time, the suspect can be arrested” (SSP, 2020, translated by the author).

[66] No information was found about the data-base.

[67] This action reinforces the notion of panopticism developed by Foucault, which highlights the use of surveillance and monitoring in institutions, specifically in prisons.

[68] “Among the equipment purchased are 07 pieces of software designed to record, display, retrieve and send alerts; 99 cameras, 68 of which have a night image range of 60 meters to 90 meters; 10 equipped with infrared; 15 cameras with motion detection, and 6 with facial recognition” (SESP, 2023)

In the context of imprisonment, Minas Gerais has implemented the Biomtech facial recognition system since 2018 for the registration and tracking of sentenced individuals[69], including those under house arrest and conditional suspension of sentences and legal proceedings. Over seven thousand sentenced individuals have been registered in the system.

In Paraná, cities like Curitiba and Maringá have been notable for their adoption of facial recognition technology in public safety. Curitiba's "Projeto Muralha Digital"[70], launched in June 2020, introduced 488 video surveillance cameras equipped with facial recognition capabilities, panoramic views, thermal imaging, and license plate recognition in strategic locations throughout the city. Maringá was recognized as the smartest city[71] in the state in 2021 and introduced its Integrated City Control Center in 2022, which features facial recognition capabilities, license plate recognition, data processing software, forensic analysis tools, and big data capabilities (FGV Direito Rio, 2022).

Bahia deserves attention due its pioneering the experimental use of facial recognition technology in the country in December 2018[72]. Currently, 78 municipalities in Bahia utilize facial recognition, license plate recognition, and situational analysis services, managed by the State Secretary of Public Security (SSP). The System of Facial Recognition of the Secretary of Public Security of the State is given the credit of locating around two fugitives from justice per

[69] The facial recognition implementation in Mineirão, a football stadium in the State of Minas Gerais, follows a panoptic framework, once it aims to "inhibit" supporters to perform violent acts, therefore, molding their "behavior". If the rule is not followed, legal measures are taken. See more information in: https://www.uol.com.br/esporte/ultimas-noticias/enm/2022/03/04/mineirao-tera-estreia-de-ferramenta-de-reconhecimento-facial-no-classico-entre-atletico-mg-e-cruzeiro.htm

[70] For more information on the project, access the link: https://muralha.digital/

[71] On the classification of a smart city, the Report on the expansion of AI Surveillance, Steven Feldstein (2019) describes the category as those cities with sensors that transmit real-time data to facilitate service delivery, city management, and public safety. They incorporate diverse tools, including facial recognition, which are connected to an intelligent command center.

[72] Further insights on the case of FR and surveillance technology implementation in Bahia is provided the report entitled "O sertão vai virar mar: expansão do reconhecimento facial na Bahia", developed by "O Panóptico" , available at: https://opanoptico.com.br/wp-content/uploads/2023/08/O_sertao_vai_virar_mar-expansao_do_reconhecimento_facial_na_Bahia.pdf

day[73] (Governo do Estado da Bahia, 2023). However, the enthusiasm with the results of the applicability of the technology must be contrasted by the false-positive result[74], which has led several innocent people to jail since its implementation in 2018 (Alencar, 2023).

The media has brought to light the inherent inaccuracies associated with facial recognition technology, a phenomenon not restricted to a single geographic region. To illustrate, beyond the instances observed in Bahia, an incident in the Civil Police Programme of the Federal District erroneously implicated an individual as the perpetrator of a crime, leading to his unwarranted incarceration (Bonfim, 2021). Furthermore, the Military Police of Rio de Janeiro's facial recognition system also exhibited shortcomings, resulting in the erroneous arrest of a woman (G1, 2019). These occurrences, rather than isolated anomalies, form part of a broader context. This juxtaposition underscores the multifaceted ethical and pragmatic dilemmas surrounding the deployment of facial recognition technology in the domain of public safety, transcending geographical boundaries within Brazil.

Brazilian states and municipalities[75] have increasingly invested in the implementation of video monitoring technologies[76]. This includes the creation and expansion of urban camera infrastructure, the purchase of artificial intelligence software for facial and license plate identification and recognition, as well as the creation of industry camera sharing platforms. In this context, the Optical Character Recognition, which consists of technology applied to recognize text within images, such as photos and documents digitized. It is used to convert

[73] According to the official webpage of the Civil Office, the number of fugitives from justice located with the support of the Facial Recognition System of the Public Security Secretariat (SSP) grew by 1,218% in 2023, compared to last year. Data shows that arrests increased 12-fold

[74] The term "false positive" refers to the error produced in the face capture process of the face when it is crossed with the information available in the database accessed by the system. database accessed by the system. In other words: the system detects a positive correlation between the image and the database, but the person recognized is not the one sought.

[75] According to the FGV (2023) Report, facial recognition technology is confirmed to be in use across 12 states. However, when examining the map on page 58, it suggests that its application is primarily concentrated in the municipalities of Rio de Janeiro and São Paulo, not in the State of those cities in general.

[76] Facial and vehicle license plate recognition are tools highly dependent on the functionali ty of video surveillance also related to the monitoring of objects and persons. This statement also accuses a weak classification of those technologies by Instituto Igarapé in their report.

virtually any type of image containing text, whether typed, handwritten or printed, in data versions machine readable. One potential application lies in the realm of vehicle license plates, wherein the technology discerns characters, converts the textual content, and subjects it to cross-referencing with law enforcement databases to identify patterns, specifically relating to infractions. Consequently, if information from a license plate is captured, and any irregularity is detected, such as license plate tampering, traffic violations, thefts, or robberies, a real-time alert is triggered through the integration of data with the database (FGV Direito Rio, 2023).

Among 27 federal unities in Brazil, the report of FGV (2023) identifies 12 using OCR, being them: in the northern region, Amazonas and Pará; in the central-west region, Mato Grosso, Mato Grosso do Sul and Goiás; in the southeast region, São Paulo, Minas Gerais, Rio de Janeiro and Espírito Santo; and in the southern region, Paraná, Santa Catarina and Rio Grande do Sul.

For instance, the State of Pará has implemented Optical Character Recognition (OCR) technology as part of its strategy to address issues related to violence and criminality within the region. Within this context, the state utilizes the Integration of Records for the Identification of Suspects (IRIS) system, which employs video surveillance cameras to capture and analyze information from motor vehicle identifications. Presently, this database is continuously integrated with the Ministry of Justice's national Córtex system[77]. This integration encompasses not only the cameras within the state's public security apparatus but also extends to cameras operated by the National Department of Transport Infrastructure (DNIT), federal agencies, and

[77] This is an artificial intelligence technology that uses the reading of vehicle license plates by thousands of road cameras spread across highways, bridges, tunnels, streets and avenues across the country to track moving targets in real time. The Ministry of Justice and Public Security defines it as a tool applied "exclusively for public security purposes". According to UOL News, in practice, the Córtex system allows investigators to discover where a person has traveled, as long as the car used in the trips is known, therefore, it is possible also to access the person's personal data, while the Cortex stores the information captured for a period of ten years. See more in: https://noticias.uol.com.br/politica/ultimas-noticias/2022/01/21/cortex-programa-governo-vigiar-cidadaos-crusoe.htm

even municipal bodies. This comprehensive integration enables the cross-referencing of data, facilitating the precise identification and retrieval of pertinent information (Saavedra, 2021).

Despite the widespread availability of OCR software across Brazil, there has yet to be a comprehensive investigation into the effectiveness of these systems in deterring and decreasing various criminal activities, such as vehicle infringements and the use of vehicles for illicit purposes. The main measure of success has been the quantity of identified and confiscated vehicles for example, still not balanced with the number of failures in the system.

Continuing the mapping of the use of technology in the security sector within Brazil, drones take part in this framework. By definition, drones are Unmanned Aerial Vehicles (UAV), small or large aircraft size that, as suggested by the name, does not have passengers, pilot or crew on board. Drones are controlled remotely and, despite having been developed for military purposes, today integrate multiple activities such as photography, policing, urban and border surveillance and among other functions (Instituto Igarapé, 2022). Drones are used to monitor risk areas and georeference to, filming and photography of territorialities and suspicious people, searches in areas difficult to access, such as forests and urban communities, persecution during escape of vehicles or even capturing routes and identifying signs, places and people (FGV Direito Rio, 2022).

In the pursuit of comprehensively evaluating the deployment of drones in various Brazilian states, it is imperative to acknowledge the fluidity of this dynamic landscape. The initial dataset derived from the most recent FGV Rio report in 2022 served as a foundational reference point, revealing the presence of drones across 18 federal entities. These entities include Acre, Amazonas, Rondônia, Pará, Piauí, Ceará, Alagoas, Bahia, Mato Grosso, Mato

Grosso do Sul, Goiás, the Federal District, São Paulo[78], Minas Gerais, Rio de Janeiro, Espírito Santo, Paraná, and Rio Grande do Sul[79].

However, subsequent investigations have unveiled a more nuanced picture, offering valuable insights into the ever-evolving nature of drone usage in the country[80]. Subsequent investigation has yielded additional insights into the prevailing circumstances as of the year 2023. Notably, the State of Amapá, which was not featured in the aforementioned report, had taken significant steps by the conclusion of 2022. During this time frame, Amapá had procured drones for various law enforcement agencies, including the Military Police (PM/AP), Civil Police (PC/AP), Tactical Air Group (GTA), Military Fire Department (CBM/AP), and the Scientific Police. Furthermore, in the year 2023, the state acquired nine high-precision surveillance drones through a federal government initiative (Morais, 2022; Bittencourt, 2023). Similarly, drones have emerged as valuable assets for law enforcement operations in the State of Maranhão. The Civil Police of Maranhão has emphasized the significant benefits of this technology in addressing a wide range of situations, including preventive and punitive law enforcement operations, intelligence gathering, as well as policing activities conducted during public events (Polícia Civil do Maranhão, 2023).

[78] In relation to the use of drones, the report Segurança Pública na Era do Big Data of FGV Rio (2022, p.73, translated by the author) it is identified that “the Government of the State of São Paulo, through the Secretariat of Public Security, started the "DronePol " project in 2019, focusing on equipping and preparing the military, civil and technical-scientific police to use this tool in civil defense and public security activities. The project investment of 6.3 million reais and takes into account the operational of flying in hostile and confined environments, without exposing human lives, as well as other human lives, as well as other aspects relevant to intelligence missions (Pedrezani, 2019).

[79] “In the northern region, Acre, Amazonas, Rondônia and Pará. In the northeast, Piauí, Ceará, Alagoas and Bahia. In the center-west region, all use it, Mato Grosso, Mato Grosso do Sul, Goiás and the Federal District. In the southeast, all of them use it, São Paulo, Minas Gerais, Rio de Janeiro and Espírito Santo. And in the South, only Paraná and Rio Grande do Sul” (FGV Direito Rio, 2022).

[80] Through research, it was observed that drone technology has been utilized for security purposes in states such as Paraiba and Pernambuco. However, this usage was not included in the report, and there were no findings on the continuation of such practices in these cases. Additionally, no information was found regarding the employment of drones in other states, such as Rio Grande do Norte. For more details on the Paraíba case, please visit https://www.pm.pb.gov.br/portal/2021/09/29/em-feira-de-inovacao-policia-militar-expoe-ferramentas-tecnologicas-que-tem-auxiliado-corporacao-no-combate-a-criminalidade-na-paraiba/ . Further information on Pernambuco can be found at https://g1.globo.com/pe/pernambuco/noticia/2018/09/21/drones-passam-a-auxiliar-acoes-de-seguranca-publica-em-olinda.ghtml.

Such findings are instrumental in elucidating the transformative nature of technology adoption in some states. However, the challenge of information availability persists, with certain states remaining uncharted territory due to the absence of updated sources. This underscores the need for continued vigilance and exploration, as the landscape of drone usage in Brazilian states continues to evolve, leaving certain regions in a knowledge void and warranting further inquiry.

Similarly, body cameras have gained prominence as a technological tool widely embraced by numerous police forces. Referred to also as uniform cameras, wearable cameras, individual cameras, body cams, body-worn cameras. The use of these devices is accompanied by a discourse in which technology is seen as a more professional, rational and efficient practice of public security agents (Lima et al., 2022). In the Panorama Collection launched by Panóptico, a project of the Center for Security and Citizenship Studies (CESeC), body cameras were a presented technology which functionality was defined as:

> "A body camera is a video and audio recording device that is most often attached to police uniforms. The video is usually saved with information (meta-data) on date, time and GPS coordinates. Some body cameras offer streaming video in real time. those that offer automatic recording options, while others need to be triggered by the police officer to start recording. recording. The images generated by the cameras are stored in external databases maintained by police agencies or third-party suppliers" (Lima et al., 2022, translated by the author).

In Brazil, the application of this technology spans a wide spectrum of practices, ranging from non-existence to pilot projects, ongoing implementation processes, and active utilization. The initial adoption of body-worn cameras within Brazilian law enforcement marked a four-year journey, commencing with the implementation by Santa Catarina. As of now, the majority of Brazilian states have either incorporated these devices into their operations or are actively assessing and experimenting with their deployment.

Findings from the Violence Monitor survey indicate that portable operational cameras are in use to varying extents among police forces in 7 states, collectively representing 25% of the country's federative units. These states include Minas Gerais, Pará, Rio de Janeiro, Rio Grande do Norte, Rondônia, Santa Catarina and São Paulo. For instance, São Paulo, in particular, stands out as the leader in this endeavor, with an inventory exceeding 10,000 cameras, constituting 52% of its operational police personnel (Velasco et al., 2023).

Furthermore, 10 states report being in the process of adopting body-worn cameras, however at different stages. Some are in the preliminary stages of drafting procurement calls for the acquisition of equipment, while others have advanced to the bidding phase or are actively conducting camera trials. Nine additional states are situated at even earlier stages, engaging in feasibility assessments and evaluations concerning the use of these cameras[81]. (Velasco et al., 2023).

In the context of technological adoption within law enforcement, the underlying motivations often revolve around the aspiration to downsize the inappropriate use of force, reinforce mechanisms of control, and enhance operational efficiency. This multifaceted purpose can be construed as a dual-edged sword, encapsulating both a deterrence mechanism and an instrument of surveillance[82]. This deterrence facet operates twofold: it serves as a

[81] The use is made by Minas Gerais, Pará, Rio de Janeiro, Rio Grande do Norte, Rondônia, São Paulo and Santa Catarina. In the bidding or testing phase are found Acre, Alagoas, Amapá, Bahia,Espírito Santo, Paraná, Pernambuco, Piauí, Rio Grande do Sul, and Roraima. Finally,
Amazonas, Ceará, Distrito Federal, Goiás, Mato Grosso, Mato Grosso do Sul, Paraíba, Sergipe, and Tocantins have it under evaluation. Maranhão stands as the sole state that has not initiated camera use (Velasco et al., 2023).

[82] In essence, the use of body cameras can be seen as a manifestation of disciplinary techniques, where surveillance and evidence play a pivotal role in regulating and controlling the behavior of individuals within a societal framework, echoing Foucault's insights into the workings of power and discipline in contemporary institutions.

potential deterrent against police officers' abusive conduct while concurrently mitigating aggressive behavior directed towards law enforcement during civilian interactions.

In this regard, body-worn cameras are composed to amplify the supervisory capacity of law enforcement supervisors. This, in turn, is expected to augment compliance with established protocols and instill greater restraint among police personnel. Simultaneously, the intrinsic capacity of body cameras to generate higher-quality, more reliable evidence holds the potential to elevate the likelihood of legal proceedings against law enforcement officers implicated in unlawful or abusive conduct. Such legal action serves as a pivotal component in the broader framework of accountability and transparency within the criminal justice system (Magaloni et al., 2022).

Concerning some benefits and dangers of the use of this technology, Magaloni et al. (2022) illuminate a dual perspective that encompasses both transformative potential and inherent risks. These perspectives diverge notably. On one hand, body cameras are heralded as a "revolution" in policing, engendering transparency through heightened control and oversight of law enforcement actions and operations. On the other hand, they possess the capacity to institute systematic surveillance of individuals categorized as "risk factors," often labeled as "suspicious elements," and potentially extend this surveillance to the broader public.

Nonetheless, the actualization of transparency through body cameras remains uncertain. Velasco et al. (2023) reveal instances that challenge that notion of transparency by presenting two different cases that corroborate the idea. Firstly, the occurrence of one of the most lethal operations in São Paulo’s police history, in which only 6 out 16 fatalities were captured by the equipment[83]. The justification provided was that either the cameras were not loaded or were experiencing technical malfunctions. Similar issues with equipment functionality have been

[83] For further information on the case, access the link https://g1.globo.com/sp/sao-paulo/noticia/2023/08/03/bos-apontam-que-apenas-uma-equipe-da-pm-usava-cameras-em-11-mortes-da-operacao-escudo-na-baixada-santista.ghtml

documented in Rio de Janeiro, where the State Public Defender's Office reported a success rate of merely eight out of ninety requests to the Military Police for access to body camera footage[84]. Notably, these requests were made after the expiration of the stipulated image storage period.

Moreover, complexities arise in the realm of equipment ownership and management. Some states opted for leasing or borrowing the cameras, while others made outright purchases. This discrepancy in acquisition models introduces uncertainties regarding operational understanding and logistics, such as maintenance protocols and technology updates, which are imperative given the rapid evolution of camera technology. The absence of clarity concerning the management of these cameras, including chain of custody practices, poses additional concerns.

Furthermore, the potential application of biometric analyses, particularly facial recognition, to the records generated by body cameras introduces further apprehensions (Lima et al., 2022). These considerations highlight the multifaceted nature of body-worn camera deployment within law enforcement, necessitating a comprehensive examination of their implications and operational dynamics in the pursuit of effective and ethically sound practices.

Data plays a fundamental role as a tool in shaping the scene of current law enforcement efforts, the development of sophisticated algorithmic models enabled a revolutionizing policing operations and tactics[85]. This transformative approach is encapsulated by the concept of predictive policing, a multidisciplinary fusion of cutting-edge technology, criminological theory, and predictive algorithms[86], as elucidated by Selbst (2017). Predictive policing

[84] For further information, access the link https://g1.globo.com/rj/rio-de-janeiro/noticia/2023/08/27/em-relatorio-ao-stf-defensoria-publica-indica-problemas-em-cameras-usadas-pela-policia-militar-do-rj.ghtml

[85] In her book "Weapons of Math Destruction", O'Neil argues that prediction can be applied in different contexts, whether through computer programs or mental processes. These models utilize our existing knowledge to anticipate outcomes in different contexts, and we all possess numerous models that inform our expectations and guide our decision-making. O'Neil writes (2016, p.23): “Whether it’s running in a computer program or in our head, the model takes what we know and uses it to predict responses in various situations. [Models] tell us what to expect, and they guide our decisions”.

[86] Further definition and discussion on predictive policing can be found in the text “Disparate impact in big data policing” written by Selbst (2017).

therefore represents the convergence of data and analytics to proactively anticipate and forecast criminal activities.

While the concept of forecasting crime is not entirely new within the realm of security and law enforcement, considering the existence of crime mapping and profiling methods for example, the true novelty of predictive policing lies in the era of Big Data. As Selbst (2017) observes, the advent of vast, complex datasets has introduced a new era of law enforcement strategies, where the potential for data-driven decision-making is vast.

Predictive policing lies in the art of data mining, a process through which correlations between criminal outcomes and a multitude of input data are unearthed. The author clarifies that "predictive policing uses data mining methods to find correlations between criminal outcomes and various input data they have collected—crime locations, social networks, or commercial data" (Selbst, 2017, p.113). The mining of these intricate relationships allows law enforcement agencies to not only gain a deeper understanding of criminal patterns but also to proactively allocate resources and deploy tactics in a manner that maximizes the prevention and mitigation of criminal activities.

Currently, there exist numerous tangible criminological uses for predictive analysis, a method involving the statistical examination of extensive historical data to forecast upcoming criminal occurrences or developments. The applicability in predicting policing can range from forecasting offenders, projecting potential victims, and predicting the times and locations with an elevated likelihood of fresh criminal incidents (FGV Direito Rio, 2022; Perry et al., 2013). In this context, Hardyns e Rummens (2017, p.203) categorize predict policing as follows:

> "The first category consists of, for example, the prediction of recidivism (Berk et al. 2009) or the identification of possible perpetrators based on their background and the characteristics of certain crimes. In these cases, predictive analysis complements other methods such as (geographic) profiling. The second category is aimed at, for example, predicting which people

> are at risk of becoming a victim of a certain crime based on the known victims' data or the risk of the escalating of domestic or gang violence (Ratcliffe and Rengert 2008). The objective of the third category is to predict future crimes as precise as possible in time and space and use that information to proactively guide police patrol routes or the locations of police controls."

In Brazil, the controversy surrounding the implementation of predictive policing has led to challenges in categorizing law enforcement institutions operating within this framework. Consequently, distinguishing states or governmental entities engaged in predictive policing remains an imprecise task. Oliveira de Moraes (2022) argues in favor of the existence of sparse systems, thereby complicating the country's classification within a consolidated framework. Nonetheless, the author identifies projects that exhibit elements of predictive policing. This classification ambiguity further hinders the identification of states with well-established predictive policing initiatives, leading to a divergence of opinions among experts. Rio de Janeiro, Ceará, and São Paulo are included in this context by some, while others exclude them[87].

In the case of Rio de Janeiro, the Civil Police of the State was identified by The Intercept Brasil as a client of the multinational Oracle, that sold softwares of data analysis for police forces [88] (Dias & Hvistendahl, 2021). The technology was offered to police authorities in the

[87] Oliveira de Moraes (2022) identifies two projects, one in the national level, entitled Cortex; and the other Detecta from São Paulo. Ceará and Rio de Janeiro are mentioned in the work Segurança Pública Datificada e Policiamento Preditivo (2022) and in the report Segurança Pública na Era Digital elaborated by FGV (2022). The second document only identifies São Paulo and Ceará as users of technology with web scrapping.

[88] In the investigation conducted by The Intercept Brazil, a slide containing the technology offered to the Rio Civil Police was found, similar to software such as Palantir and PredPol, which promise to predict crimes. The media found 3 active contracts with Oracle, after searching on Transparency Portal, although the Civil Police denies the existence of them.

context of mega-events[89] and security enforcement[90] (Dias & Hvistendahl, 2021). In this scenario, the technology was able to bring together different databases, organize and hierarchize information such as: police occurrences, firearms, cell phones, vehicles, people and even biometric biometric data, facilitating access for police officers and optimizing resources (FGV Direito Rio, 2022).

In Ceará, the Sistema Tecnológico para Acompanhamento de Unidades de Segurança[91] (Status) was launched in 2021, consisting of the use of analytical intelligence for criminal data, using data science, statistics, geoprocessing and artificial intelligence which allows the identification of "criminal spots", and the development of strategies towards that (Secretaria da Segurança Pública e Defesa Social, 2021).

In São Paulo, the Secretariat of Public Security of the State developed DETECTA, which is an integrative system of information that performs the correlation of this information to assist the decision-making by the military, civil and scientific police (Secretaria de Segurança Pública do Governo do Estado de São Paulo, 2017). Aiming to assist the police in operational and investigative activities, the process consists in accessing databases from different institutions[92]; correlating information and images of places, people and vehicles; and

[89] In August 2016, Instituto Igarapé partnered with Via Science developed CrimeRadar platform, which was "a public-facing crime forecasting platform that evaluated relative crime frequencies in different locations and times of metropolitan Rio de Janeiro. The underlying crime data was retrieved from the state Institute for Public Safety and included official crime records produced by the state civil police" (Aguire et al., 2019) Therefore, the platform aim is under the third category identified by Hardyns e Rummens (2017). Additionally, the partnership with governmental institutions is also mentioned in the report "Starting in 2018, the Institute partnered with the State Military Police of Santa Catarina to develop and pilot a police-facing version of CrimeRadar." This case was not mentioned in any bibliography referring to predictive policing in Brazil.

[90] According to The Intercept Brazil, it occurred due to the World Cup in 2014, and Rio Olympic Games in 2016, which reinforces the idea of securitization and techno-solutionism presented in this thesis work. See above pages. "At the time of the World Cup, in 2014, and the Olympics in Rio de Janeiro, in 2016, Brazil was experiencing the height of its fetish for security technologies. Governments were eager to show service and prove to the world that Brazil was, indeed, a safe place to receive tourists. At that time, Rio de Janeiro created the Integrated Command and Control Centers, which gathered information from the police forces and made the security industry swim in public money. Drummond, at the time, was an advisor to the Rio de Janeiro police command and also a member of the committee responsible for strategic planning for mega sporting events. It was in this context that Oracle's solutions were presented to the Civil Police" (Dias & Hvistendahl, 2021)

[91] In English, Technological System for Monitoring Security Units.

[92] The official website from the São Paulo Government announced that "In addition to camera monitoring, Detecta brings together the largest database of police information in Latin America. The databases of the civil and military police, the Digital Record of Occurrences (RDO), the Identification Institute (IIRGD), the Military Police

promoting coordinated police actions (Secretaria de Segurança Pública do Governo do Estado de São Paulo, 2017).

In conclusion, the dynamic evolution of the interface between technology and national security in Brazil has become evident. As we have explored the utilization of surveillance technologies by law enforcement agencies and military forces, it becomes evident that facial recognition, body cameras, drones, and optical character recognition are at the forefront of these advancements. These technologies have been adopted by various states and municipalities, with notable examples including Bahia, São Paulo, and Rio de Janeiro. However, this progress is not without its challenges and ethical dilemmas. As technology continues to evolve, the need for comprehensive evaluation, transparency, and ethical considerations becomes paramount.

Operational System (SIOPM-190), the Criminal Photo System (Fotocrim), as well as vehicle data and National Driving License (CNH) from Detran. The data brings together information and photos of wanted criminals, records of missing people, data on the status of vehicles, whether their documents are in order, whether they have been stolen, stolen or cloned. Images from private cameras are also used in police operations, which are analyzed and screened by company employees. Images related to police incidents are sent to the database in the form of alerts. They are recorded and stored where they were recorded and can be requested in the event of police or military action." See more in https://www.saopaulo.sp.gov.br/spnoticias/detecta-monitora-o-estado-de-sao-paulo-com-3-mil-cameras-de-video/

CHAPTER 3

Data governance: ethical and legal dimensions

The incorporation of these advanced technologies within the public security sector has brought proeminence to ethical and legal challenges. These challenges have come into sharp focus amidst the dynamics of data collection, processing, and analysis. At the heart of this multifaceted issue lie the paramount concerns surrounding bias, privacy, fairness, and accountability. The integration of surveillance technologies into security operations has fundamentally transformed the way data is collected, utilized, and interpreted, necessitating a comprehensive examination of the legal and ethical dimensions intertwined with these advancements.

Moreover, as the relationship of these tools with public safety and security is increasing, the need for robust legal frameworks to govern their usage and safeguard individual rights has become more imperative than ever before. In this complex landscape, it is essential to scrutinize how these technologies impact bias, privacy, challenge notions of fairness, and demand elevated accountability, while simultaneously ensuring that they are leveraged in a responsible and ethical manner.

3.1 Ethical complexities of surveillance technologies in Brazil's security scenario

The advancement in surveillance technologies stages an in-depth exploration of ethical complexities in Brazil's surveillance environment. Addressing the pressing challenges in the realm of public security starts with the relationship between private technology corporations and public security operations, which has ushered in a new era of enhanced law enforcement capabilities.

Private technology corporations play a significant role in shaping the discourse around enhanced law enforcement capabilities. The promotion of smart solutions creates a sense of connected and secure cities globally, including in Brazil, where technological support to law enforcement agencies and empower community organizations with surveillance capabilities is provided. The adoption of surveillance and security technologies is often a collaborative effort between public and private entities.

These technologies, which are increasingly pervasive in urban environments, frequently originate from foreign sources. The primary avenues for technology acquisition include cooperation agreements, equipment donations, and electronic procurement processes. For instance, many cases involving public security technology, such as facial recognition systems, have a significant presence of Chinese companies, including Dahua, Hikvision, and Huawei[93] (Reis et. al, 2021). Furthermore, in the context of smart cities, facial recognition, and smart policing in Brazil, the Global Surveillance Index identified Axis, Dahua, and IBM as key companies (Feldstein, 2019).

This intertwined relationship between public and private entities blurs the lines between public services and commercial practices, raising questions about the extent to which technology itself can ensure security versus the sociotechnical practices behind it[94].The ramifications of an imbalanced commercial relationship between governments and corporations can manifest in various ways, and this issue extends beyond the technology sector. It is evident that the involvement of private enterprises in urban management raises numerous

[93] For instance, the report elaborated by FGV (2022) presents that the city of Campinas initiated the incorporation of facial recognition technology and additional security components as part of the "Cidade Segura Campinas" project, which in pilot phase was a collaborative effort involving the municipal government, the Chinese company Huawei, and the Research and Development Center in Telecommunications (CPQD).

[94] "The problem involving the provision of technological solutions by companies to governments concerns the ability of these corporations to guide the public agenda and urban planning models" (Branco, 2019, translated by the author) In: Branco, P. (n.d.). Smart Cities como dispositivos biopolíticos. VI Simpósio International LAVITS 2019, Salvador, Brazil. https://lavits.org/wp-content/uploads/2019/12/TeixeiraBlanco-LAVITISS-2019.pdf

concerns within the so-called “Smart Cities”[95], which is described by Feldstein (2019, p.16) as those “with sensors that transmit real-time data to facilitate service delivery, city management, and public safety”, being also “referred to as ‘safe cities’, they incorporate sensors, facial recognition cameras, and police body cameras connected to intelligence command centers to prevent crime, ensure public safety, and respond to emergencies”[96].

In the pursuit of smart city initiatives and governance, big tech companies are getting involved in managing different aspects of city dynamics. According to Rob Kitchin (2014), it becomes evident that the involvement of major tech companies in city management poses significant challenges due to profit-orientation practices, technological lock-ins[97], and standardization of smart cities format[98]. The corporatization of urban governance, fueled by the adoption of technology for monitoring and regulating various aspects of city life, raises concerns about private profit-driven motives, intensifying the discussion on techno-solutionism. Besides, the increasing reliance on specific technological platforms creates a potential for monopolies and long-term dependence, limiting the flexibility of cities to adapt or switch to alternative solutions. Finally, the tendency towards standardized, one-size-fits-all smart city solutions may overlook the unique needs of communities and cultures, potentially

[95] By definition,”The World Bank describes smart cities as ‘technology-intensive’ urban centers featuring an array of sensors that gather information in real time from ‘thousands of interconnected devices’ in order to facilitate improved service delivery and city management” (Feldstein, 2019).

[96] “IBM, one of the original coiners of the term, designed a brain-like municipal model where information relevant to city operations could be centrally processed and analyzed. A key component of IBM’s smart city is public safety, which incorporates an array of sensors, tracking devices, and surveillance technology to increase police and security force capabilities (...) Huawei has been up-front about trumpeting public safety technologies for smart cities. It is marketing “safe cities” to law enforcement communities to “predict, prevent, and reduce crime” and “address new and emerging threats” (Feldstein, 2019, p.17).

[97] Potentially creating monopolies and corporate path dependencies that are challenging to reverse (Rob Kitchin, 2014).

[98] For instance, the aforementioned IBM offers a product called 'Intelligent Operations Center' that bundles together systems initially made for Rio de Janeiro and can be used in any city. In the New York Times interview, the I.B.M.’s chief technology officer of the global public sector said: “I have seen better infrastructure in individual departments in other cities,” said Mr. Banavar (...) “But I haven’t seen this level of integration in other cities’”See more in https://www.nytimes.com/2012/03/04/business/ibm-takes-smarter-cities-concept-to-rio-de-janeiro.html

reinforcing surveillance-oriented governance models. All those factors intensify the risks of surveillance and data misuse.

Moreover, the Smart Sampa project[99], aligned with the broader concept of smart cities, represents a case of concern within the Brazilian context. Since it was launched in 2022, the project has been the target of a series of questions, including from the Municipal Audit Court, about data collection and information sharing[100] (Arcoverde, 2023). This case exemplifies the tensions arising from the rapid deployment of surveillance technologies in smart cities and the necessity for their robust oversight.

The dramatic increase in public surveillance and intrusive security capabilities noticed by Feldstein (2019) aligns with the findings exposed in the LAPIN report (2021), which concludes that certain instances involve technology suppliers having extensive access to the personal data being processed, with no provisions or agreements found concerning the transfer of technological knowledge to public authorities[101] (Reis, et. al., 2021).

Taking these facts into account, Priscila Branco (2019) suggests that it is necessary for governments to propose compensations and clear rules to the companies they hire, precisely to legally address sensitive areas. Moreover, Shoshana Zuboff (2015) warns that the rapid growth of surveillance technologies, without adequate public understanding and legal regulations, has

[99] In August 2023, The mayor of São Paulo signed a contract to initiate the Smart Sampa Project, which is considered the largest monitoring system and integrated technologies programs. The official webpage of the city government, through its Communication Special Secretariat published the following news explaining the project, its goals and implementation: https://www.capital.sp.gov.br/noticia/prefeito-assina-contrato-para-o-inicio-do-smart-sampa-maior-programa-de-videomonitoramento-da-cidade-com-ate-40-mil-cameras-2

[100] The Intercept Brazil published an investigation of the Smart Sampa project, providing information on the consortium process, the companies involved, and corruption accusations. The entire investigation can be found on the link: https://www.intercept.com.br/2023/08/14/smart-sampa-denunciada-por-corrupcao-capturar-seu-rosto-em-sp/ Moreover, in May 2023, the São Paulo Government released a press note entitled "City Hall Overturns Injunction And Resumes Public Tender To Install 20,000 Security Cameras In The City" . The entire text is available at https://imprensa.prefeitura.sp.gov.br/noticia/prefeitura-derruba-liminar-e-retomara-edital-para-implantar-mil-cameras-de-seguranca-na-cidade

[101] "In some cases, the companies supplying the technology have broad access to the personal data processed; No provision or agreement was identified regarding the transfer of knowledge about the technology to the public authorities" (Reis, et. al., 2021, p.27 , translated by the author).

allowed surveillance for profit to flourish. Ironically, Privacy rights can be used as a shield to justify these practices while keeping the operations themselves hidden from public scrutiny[102].

The utilization of the "multifunctionality criterion" implies that data gathered for public security may be redirected for alternative purposes[103] (Rodotà, 2009, p 78). This raises concerns about the transparency of data origins initially collected for specific security objectives, potentially ambiguity regarding the original intent of data collection. There exists a potential risk in surveillance technologies where profit motives overshadow public security concerns[104] (Rodotà, 2009; Zuboff, 2015). Once more, this scenario poses implications for public security, prompting inquiries into the transparency and accountability of surveillance operations conducted ostensibly for security purposes.

In examining the intricate relationship between public and private entities in the realm of technology acquisition and utilization, it becomes evident that the convergence of commercial interests and public services gives rise to multifaceted challenges. It is crucial to recognize the consequences of an imbalance of data access and management. The smart cities projects towards surveillance for security purposes highlight the need for robust management and regulatory frameworks in the face of rapid surveillance technology deployment.

[102] "Surveillance capitalists have skillfully exploited a lag in social evolution as the rapid development of their abilities to surveil for profit outrun public understanding and the eventual development of law and regulation that it produces. In result, privacy rights, once accumulated and asserted, can then be invoked as legitimation for maintaining the obscurity of surveillance operations" (Zuboff, 2015, p.83)

[103] "In this manner, some of the principles underlying the system of personal data protection are being slowly eroded; this applies, first and foremost, to the purpose specification principle and the principle concerning separation between the data processed by public bodies and those processed by private entities. The multifunctionality criterion is increasingly applied, at times under the pressure exerted by institutional agencies. Data collected for a given purpose are made available for different purposes, which are considered to be as important as those for which the collection had been undertaken. Data processed by a given agency are made available to different agencies. It means that individuals are more and more transparent and that public bodies are more and more out of any political and legal control. It implies a new distribution of political and social powers" (Rodotà, 2009, p.78)

[104]"The fundamental right to data protection is continuously eroded or downright overridden by alleging the prevailing interests of security and market logic." (Rodotà, 2009, p. 8). Additionally, "Surveillance capitalists have skillfully exploited a lag in social evolution as the rapid development of their abilities to surveil for profit outrun public understanding and the eventual development of law and regulation that it produces. In result, privacy rights, once accumulated and asserted, can then be invoked as legitimation for maintaining the obscurity of surveillance operations" (Zuboff, 2015, p. 83).

The surveillance ubiquity towards the security sphere brings deep dilemmas in many sensitive areas, such as privacy, algorithmic bias and controlling mechanisms, which underscore the urgency of striking a balance between technological progress, data protection, and effective governance. As the focus shifts to data in the following paragraphs, it becomes clear that addressing these issues is essential to safeguard rights and ensure ethical technological advancements.

The growing presence of surveillance technologies in Brazil is concentrated in security purposes which depends on the data collection for efficient implementation[105]. Consequently, the classification of data into categories is fundamental here as it serves as basis for a more profound comprehension of the intricate techniques involved in the process[106]. Furthermore, in Brazil, there is a substantial collection of geolocalization, image, personal, biometric, and sensitive data, predominantly for the advancement of public security objectives[107] (Igarapé, 2022).

In the context of data classification for academic research and security applications, it is crucial to define and distinguish between various categories of data. Localization data, also known as geolocation data, refers to information that pinpoints the physical location of an individual, device, or object on the Earth's surface, including GPS coordinates and IP addresses. Image data comprises visual information in the form of digital images or photographs, used in applications like facial recognition and medical imaging. Personal data encompasses information that can identify an individual, such as names, addresses, and social security numbers, for example.

[105] Which is entangled with the private companies in the technological sector, as mentioned in the above section.
[106] In the annex number x, it is possible to find definitions of data by categories.
[107] "In general, surveillance depends on massive collection of data, be it cadastral, sensitive, biometric and/or geolocation data (...) While the transportation, public safety, education and events/tourism sectors predominate in the collection of images resulting from the widespread use of video surveillance, the health and intelligence sectors diversify the type of data collected (...) In general, there is greater diversity in the type of data collected in all sectors, especially in health and public security" (Igarapé, 2022, p.9-10, translated by the author)

Under the personal data broad category, the one resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data, is considered biometric data (EU General Data Protection Regulation, 2016). Sensitive data, on the other hand, encompasses information that discloses an individual's racial or ethnic background, religious or philosophical beliefs, political affiliations, union memberships, genetic or biometric details, as well as aspects related to an individual's health or personal sexual life (Presidência da República do Brasil, 2021). Understanding and categorizing these data types are fundamental for data governance, decision-making, and compliance with data protection regulations.

Hence, the implementation of surveillance technologies by various systems in Brazil, as discussed earlier, provides immediate access to extensive databases of information about population, in accordance with the data categorization outlined above. The constant monitoring of people allows the massive data crossing about human features and behaviors. Therefore, surveillance techniques are a “neopanopticon” symbol representing the variety of tools that captures behavioral patterns beyond images (Bordignon, 2020; Peron, 2016).

In this sense, in the context of security policies, surveillance systems have evolved to capture an significant array of information about individuals, their activities, and their surroundings. Each detail of life under surveillance systems is captured and transformed into data, which due to characteristics of volume, velocity and variety is often referred to as "Big Data"[108] (Kitchin, 2014). This has emerged as a crucial asset for the security sector, influencing the way law enforcement and related institutions act, as mapped in this work.

With the development of technologies for extraction, analysis, classification, selection, grouping and manipulation of data, it has become processable by of computers and oriented by

[108]

algorithms[109] (Peron, 2016; Rodrigues, 2022). The data processing can generally be divided into two primary phases: data mining and profiling (Peron, 2016). Data mining involves the systematic extraction of valuable information from the massive data sets collected through surveillance. Profiling, on the other hand, entails the creation of comprehensive profiles or behavioral patterns based on the mined data. This process allows law enforcement agencies to understand and anticipate certain behaviors, potential threats, and security risks. For further clarification, Peron (2016, p.9, translated by the author) describes the process as the following:

> "At first, generally public information is screened, such as identity numbers, images an d photos, license plates, residence, education, color, age, among others, and depending on the system and context, private data is called up, such as telephone and bank details, criminal records, etc."

In addition, the author explores specifically the geographical profiling:

> "The systems are also supplied with geo-referenced criminal information and data, enabling the creation of so-called density maps, which allow security agents to visualize incidents that have occurred in the past, as well as flows and spaces where citizens and criminals circulate".

Given the definition of data and their utilization in the security sector, it is important to present a critical concern that arises from the inconsistency and opacity inherent in data collection and analysis. This issue becomes particularly pronounced when considering the prevalence of "bad data"[110], which due to its inconsistency and inaccuracy, hinder the quality

[109] Peron (2016, p. 9, translated by the author) writes that "computer platforms that underpin this type of practice are characterized by complex systems for the massive collection of data, guided by algorithms for searching, classifying, selecting, grouping and crossing information". Gabriella Rodrigues (2022, p.50, translated by the author) adds that "in this way, the vast amount of data acquired has become processable in view of the data processing capacity of supercomputers and their algorithms (mathematical processes aimed at solving a certain problem), including machine learning algorithms".

[110] "What is bad data? Before answering this question we need to know the origin of the term and the purpose of the expression. (...) [it] means "incorrect data", "corrupt data", "invalid data"(Moraes, 2022, p.95 translated by the author).

of decisions (Moraes, 2022). The existence of false positives in the context of facial recognition technology, as highlighted in previous cases exposed, such as in Rio de Janeiro, exemplifies the manifestation of this bad data. These inaccuracies[111] can lead to wrong identifications and have consequences for individuals who may be wrongly accused or targeted.

Moreover, the opacity of these systems further exacerbates the problem. Often, the inner workings of surveillance technologies, including the algorithms that underpin them, remain in secrecy, making it challenging to scrutinize and rectify errors[112] (Moraes, 2022). The origins and means of technology acquisition and utilization, intersecting the public and private sectors, represents this situation. Consequently, the lack of transparency in data sources and analytical methods can perpetuate inconsistencies and bad data, casting doubt on the reliability and fairness of these systems.

In fact, the meticulous collection and processing of data, guided by advanced mathematical tools have empowered law enforcement institutions to enhance their surveillance and predictive capabilities. Firstly, the classification of data into distinct categories served as the foundation for comprehending the intricate techniques involved in these systems[113]. Surveillance technologies have evolved to capture an extensive array of information about individuals, and this abundance of data has become an invaluable asset for the security sector, influencing the way law enforcement and related institutions operate. While in theory technology is presented as an opportunistic tool for crime prevention and public safety enhancement in a country that presents high levels of criminality, in practice, this system used to surveillance and monitoring the population is accompanied by great challenges[114].

[111] For instance, "Movie star Michael B. Jordan's name appears on Ceará police's wanted list", according to G1. See https://g1.globo.com/ce/ceara/noticia/2022/01/07/astro-do-cinema-michael-b-jordan-aparece-em-lista-de-procurados-pela-policia-do-ceara.ghtml

[112] "So the problem we have is that the data, process and operation through the use of the algorithm, in practice, remains opaque, often because it is an industrial secret" (Moraes, 2022, p.98 translated by the author)

[113] Including geolocation, image, personal, biometric, and sensitive data.

[114] The system can be used for monitoring and surveillance of citizens, civil society organizations, social movements, political leaders and protesters, on an unprecedented scale (Rebello, 2020).

With the development of cutting-edge technologies for data extraction, analysis, classification, selection, grouping, and manipulation, the processing of this vast data has become feasible. However, it is essential to recognize that challenges persist, inc luding the prevalence of "bad data" and the opacity surrounding these systems. Beyond the evident demand for addressing technological improvements with efforts to minimize inconsistencies, enhance transparency, and refine data quality, it is essential to embrace a broader conversation about far-reaching implications of these technologies. It is crucial to ensure an alignment with values of fairness, accountability, and rights, surpassing ethical and practical challenges, and overcoming misuse and bias, that will be discussed in the following pages.

The discussion surrounding the framing of data and the inherent biases and challenges associated with data-driven technologies adds a critical layer to understanding of the broader implications of these systems. Afterall, they operate within complex technical considerations, as elucidated in the preceding discussion. Data extraction and analysis carry technical and functional implications once it does not exist independently from the ideas, contexts and knowledge used to generate, process and analyze them[115] (Kitchin, 2014; Moraes, 2022). In these lines, Robert Kitchin (2014, p.28) writes:

> "While many analysts may accept data at face value, and treat them as if they are neutral, objective, and pre-analytic in nature, data are in fact framed technically, economically, ethically, temporally, spatially and philosophically. Data do not exist independently. "

Additionally, in the work "Weapons of Math Destruction", Cathy O'Neil (2016) raises concerns about the role of mathematical models, once they are frequently portrayed as objective

[115] "However, impartiality is not verified when analyzing the system: there are many technical and functional problems that can reproduce discrimination rather than neutrality" (Moraes, 2022, p.98, translated by the author)

and impartial, the author contends that they are, in the contrary, shaped by human choices and intentions, as follows:

> “The math-powered applications (...) were based on choices made by fallible human beings. Some of these choices were no doubt made with the best intentions. Nevertheless, many of these models encoded human prejudice, misunderstanding, and bias into the software systems that increasingly managed our lives. Like gods, these mathematical models were opaque, their workings invisible to all but the highest priests in their domain: mathematicians and computer scientists. Their verdicts, even when wrong or harmful, were beyond dispute or appeal” (O'Neil, 2016, p.10-11)

By recognizing that data are framed and influenced by human choices, it is possible to expand the analysis through a perspective that does not neglect fairness, accountability, and rights. Compatible with the exposed ideas of Robert Kitchin (2014) and Kathy O'Neil (2016), Felipe Moraes (2022) reinforces the idea of an existence of a discriminatory bias within those systems, where impartiality is thus not verified. The author highlights the importance of data as an input for algorithmic functionality, where big data plays a fundamental role. The author underscores the substantial volume of data available, which, through processing, can be transformed into valuable insights for public security. Specifically, in the context of predictive policing, this input data consists of information related to individuals under suspicion and areas with high crime rates. Importantly, the efforts towards issues of public security is useless once biased systems are vigorous, creating and reinforcing discrimination[116].

[116] “Every algorithm needs an input, i.e. raw material to work. The main feedstock for your system is big data. In the case of predictive policing, this would be data on suspicious individuals and locations with a high incidence of crime. A huge amount of data is available which, with processing, can be transformed into useful public safety information and prevent crime from occurring, which in turn will serve as guidelines for dispatching police resources. Thus, there is no use trying to create a predictive policing algorithm that is supposedly neutral and focused on solving crime prevention if the database that feeds it has a discriminatory bias” (Moraes, 2022, p. 96, translated by the author)

Out of a total population of 203,062,512 individuals[117] 55.8% are of black according to the Continuous National Household Sample Survey from the Brazilian Institute of Geography and Statistics (DIEESE, 2022). Those numbers are significant for the debate on the quantitative dimension of discussions related to data collection and processing as well as bias for several reasons. Firstly, it highlights the substantial size of the population under consideration, which underscores the potential impact and reach of data collection efforts. Secondly, the specific percentage of the black population draws attention to the importance of understanding and addressing potential biases in data collection and processing, especially regarding racial or ethnic considerations.

For instance, in the investigative report by Intercept Brazil (2019), it was revealed that facial recognition technologies employed in law enforcement utilize facial signatures, computed based on individuals' facial landmarks, to trigger alerts. These alerts are activated when the camera captures the face of an individual with a certain degree of similarity to faces stored within the utilized database, particularly those with outstanding arrest warrants. The crucial parameter in this process is the calibration of the similarity threshold. Setting it at levels below, for instance, 90% similarity, may result in a substantial number of false positives (Nunes, 2019). Therefore, the deployment of facial recognition technology in policing contexts raises important questions regarding its effectiveness and potential consequences within a diverse societal domains, after all, those problems might result in constraints, arbitrary arrests and rights violations[118].

Furthermore, the implementation of technologies like predictive policing, which relies on facial and behavioral recognition, raises additional legal and ethical concerns. Predictive

[117] More details can be found on the provided annexes.

[118] Examples of those problems were provided in the above pages. Additionally, Pablo Nunes (2019, translated by the author) reports in the Intercept Brazil page that “During Carnival, in the four days of Micareta de Feira de Santana, in Bahia, the video surveillance system captured the faces of more than 1.3 million people, generating 903 alerts, which resulted in the fulfillment of 18 warrants and in the arrest of 15 people, that is, of all the alerts issued, more than 96% resulted in nothing”.

policing can involve "recognizing" individuals who may have committed a crime at some point in their lives, even if they have served their sentences, and placing them in a database of potential repeat offenders (Melo, 2021). Alternatively, it may label individuals as potential criminals based on specific profiles[119]. These practices not only erode individual rights but also have the potential to perpetuate discriminatory and punitive approaches within law enforcement.

In consonant with the exposed, Kathy O'Neil (2016) points out the perspective of a continuing status quo, in which the preexisting forms of discrimination which was previously performed by the police is reinforced by the utilization of those biased technologies in the public security contexts[120]. It is essential to recognize that these technologies are not inherently neutral but are shaped by the data, decisions, and societal contexts that underpin them. Consequently, these technologies may perpetuate and even exacerbate ongoing disparities in policing and security[121]. The data and the array of tools employed in the surveillance process convey an illusion of precision and impartiality that contrasts with the documented instances of injustice and violations.

[119] In the news written by Paulo Victor Melo (2021, translated by the author) for the Le Monde Diplomatique Brasil, a quotation that express this idea is brought: " 'The long racist commitment of Brazilian society is maintained by a stratification of respect for human rights, where the intersection of blackness and poverty creates preferential groups that are constant targets of surveillance and state violence – effective or always potential', highlights Tarcízio".

[120] "Needless to say, racists don't spend a lot of time hunting down reliable data to train their twisted models. And once their model morphs into a belief, it becomes hardwired. It generates poisonous assumptions, yet rarely tests them, settling instead for data that seems to confirm and fortify them. Consequently, racism is the most slovenly of predictive models. It is powered by haphazard data gathering and spurious correlations, reinforced by institutional inequities, and polluted by confirmation bias. In this way, oddly enough, racism operates like many of the WMDs I'll be describing in this book" (O'Neil, 2016, p. 26).

[121] "The result is that while PredPol delivers a perfectly useful and even high-minded software tool, it is also a do-it-yourself WMD. In this sense, PredPol, even with the best of intentions, empowers police departments to zero in on the poor, stopping more of them, arresting a portion of those, and sending a subgroup to prison. And the police chiefs, in many cases, if not most, think that they're taking the only sensible route to combating crime. That's where it is, they say, pointing to the highlighted ghetto on the map. And now they have cutting-edge technology (powered by Big Data) reinforcing their position there, while adding precision and "science" to the process. The result is that we criminalize poverty, believing all the while that our tools are not only scientific but fair" (O'Neill,2016, p.81-82)

The report "Por que eu?”[122] (2022), serves an illustrative role for this argument. Its records, analytical texts and bibliography organized between June 2021 and June 2022, found that black population in the states of Rio de Janeiro and São Paulo have a 4.5 times greater risk of suffering a police approach[123], compared to a white person (IDDD, 2022). When analyzing racial groups, it can be inferred that there is an unequal distribution and concentration of overt policing, resulting in higher levels of surveillance and control exerted over the black community.

While the primary focus of this work is not an exhaustive exploration of racism theories, it is crucial to acknowledge the existence of the challenges at hand. In this regard, racism should be recognized as a system of power that produces hierarchies, in which those at the base are classified as inferior, in need of control, or to be combated. It emerges from this perspective a combative logic, where the existence of law enforcement apparatuses is reasonable.

In this unequal system, which is theoretically sustained by Foucault (2010), racism operates as a system of power, establishing hierarchies where those at the bottom are categorized as inferior, necessitating control or even active opposition. This acknowledgment leads to a logic of conflict, suggesting that the presence of law enforcement apparatuses is justified, and neutrality is not a reality in this context.

In contemporaneity, the institutional organization is not suppressed, but perpetuated, which means that the racial logic is intrinsic to the system. The emergence of the use of technologies justified by the efficacy and efficiency for security purposes is not apart from this system. Moreover, the production of itself is imbricated with racism, which is covered by the neutral and optimal technism discourse. In essence, this acknowledgment underscores the

[122] ‘Why me?’ in English. Elaborated by IDDD and data_lab.

[123] The qualitative character of this approach is also relevant. Insights on this discussion can be found on https://iddd.org.br/wp-content/uploads/2022/07/relatorio-por-que-eu-2-compactado.pdf

intricate relationship between technology, racism, and the perpetuation of power dynamics within society.

In the Brazilian context, this matter is further exacerbated by a longstanding endorsement of racism within the societal framework. This commitment has led to a stratification of respect for human rights, where the intersection of racial identity and poverty results in certain groups becoming constant targets of surveillance and state violence, whether realized or latent. This structural racism related to surveillance technologies was critically examined by Pedro Paulo da Silva (2022), as articulated in his work:

> “In short, this produces an understanding of reality in which crime is confined to spaces where the majority of racialized populations live, which justifies the greater allocation of police forces, for example patrols, to these areas. In turn, this creates a greater likelihood of these police forces encountering historically heavily policed populations, leading to mass incarceration, police brutality and death (Camp; Heatherton, 2016; Vitale, 2017). This argument crystallizes what we call in this essay racism through technicism, because racialized policing is cloaked in the mantle of science, technocracy and management. The racial-spatial confinement maintained by the police during colonialism (Fanon, 1968) is refined through technicism” (Pedro Paulo da Silva (2022, p. 98, translate by the author).

In conclusion, the ethical challenges posed by biased surveillance technologies extend beyond technical considerations. They intersect with issues of racial discrimination, historical context, and the broader societal impact of these technologies. Recognizing the inherent biases and consequences of these tools is essential for fostering a more equitable and just approach to public security and surveillance.

3.2 Regulating surveillance: surveillance technologies and public security in Brazil

This section delves into the multifaceted landscape at the intersection of technology, security, and rights in Brazil. It critically examines the existing legal frameworks, challenges, and ethical considerations surrounding data protection, surveillance technologies, and the implications for rights and societal values. The narrative unfolds through an exploration of legislative developments, gaps in protection, and the urgent need for a comprehensive approach to reenvisioning data protection in the context of public security and surveillance policies.

The comprehensive examination of the crucial themes surrounding the intersection of technology, security and rights reveals the urgency of understanding and engagement with these pressing issues. Faced with the growing specter of neopanoptic surveillance, the challenges inherent in algorithmic biases, and the obscurity that often permeates the use of technologies, it becomes imperative to deepen the understanding of these complex phenomena and their implications. Only through knowledge and awareness can we effectively seek solutions that protect rights, promote justice and ensure that technology is a beneficial force for society.

The implementation and enforcement of data protection is greatly necessary for leaving the prevailing gaps and safeguarding citizens' rights, amplifying benefits of technology and mitigating the risks associated with it[124]. This imperative is underscored by the findings of the United Nations Conference on Trade and Development (2023) traces the data protection mechanisms and privacy legislation worldwide, pointing out that 71% of the countries in the world possess legislation concerning the theme[125], while the share in the least developed

[124] In the realm of public security, where data sensitivity extends to racial identifiers, the call for stringent protection takes on added significance.

[125] The comprehensive dataset developed by United Nations Conference on Trade and Development, including the countries with legislation and their corresponding nomenclature, can be accessed at: https://unctad.org/system/files/information-document/DP.xlsx.

countries is only 48%. This data reinforces the global disparity already discussed in this work concerning the trends of deployment and the lack of legal frameworks in the Global South[126].

In this context, Brazil holds legislation for electronic transactions, consumer protection, cyber crime, and privacy and data protection[127]. Nevertheless, the coverture of those apparatus is questionable, therefore, the country is in an ambiguous position when it comes to qualitative criteria of analysis.

In August 2018, the Brazilian General Law on Data Protection[128] entered into force. The Law 13.853 (2018) provides for the processing of personal data[129], including in digital media, by natural persons or legal entities governed by public or private law, with the aim of protecting the fundamental rights of freedom and privacy and the free development of the personality of the natural person, as expressed in its first article (Lei Geral de Proteção de Dados Pessoais, 2018).

However, all the achievements obtained with the Brazilian General Law on Data Protection do not embrace the field of public security and criminal prosecution, as exposed in art. 4, item III, paragraphs "a" and "d". Accordingly, the Law is not applicable to the processing of personal data when carried out for the purposes of public security and investigation and repression activities for criminal offenses, among other purposes, as it possible to see in the its text:

> Art. 4 This Law does not apply to the processing of personal data:
>
> I - carried out by a natural person for exclusively private and non-economic purposes;
>
> II - carried out exclusively for the following purposes:
>
> a) journalistic and artistic; or

[126] See the above pages. " This region serves as a crucible for testing emerging trends and widespread deployment of such technologies, often in contexts that lack the technical infrastructure and legal frameworks to effectively regulate them (Instituto Igarapé, 2022)"
[127] Clicking on the map corresponding to a country, it is possible to have access to that kind of legal information: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.
[128] Lei Geral de Proteção de Dados (LGPD) in Portuguese. Law 13.853.
[129] The definition of personal data can be accessed either on the aforementioned pages or at the conclusion of this work, accompanied by a table of definitions.

> b) academics, applying arts. 7th and 11 of this Law;
>
> III - carried out for the exclusive purposes of:
>
> a) public security;
>
> b) national defense;
>
> c) State security; or
>
> d) investigation and repression activities for criminal offenses (Lei Geral de Proteção de Dados Pessoais, 2018).

Although it excluded the processing of personal data for the aforementioned purposes from its scope, the Brazilian General Law on Data Protection provides that the use of data for security purposes must have its own regulations, which do not yet exist. In §1 of art. 4, it is expressed that:

> "the processing of personal data provided for in section III will be governed by specific legislation, which must provide for proportional and strictly necessary measures to serve the public interest, observing due legal process, the general principles of protection and the rights of the holder provided for in this Law" offenses (Lei Geral de Proteção de Dados Pessoais, 2018).

Furthermore, there exists a notable deficiency in safeguarding the rights of citizens due to the absence of comprehensive regulations governing the legality, transparency, and security of data processing in criminal matters. Additionally, there are no defined rights or prerequisites for utilizing emerging technologies that now enable a level of surveillance and monitoring previously unimaginable. Despite the rapid proliferation of new surveillance and investigative techniques, the absence of regulatory oversight in this domain results in a significant power imbalance between the involved parties, both the government and the citizens. In this context, data subjects are left without normative assurances and applicable institutional mechanisms to protect their personal rights, individual freedoms, and even the adherence to due process of law.

Contemplating to overcome the absence of a legal apparatus that encompasses the public security and activities involving the prosecution and repression of criminal offenses, the Commission of Jurists established by a Decree from the President of the Chamber of Deputies prepared in 2019 the Preliminary Draft Data Protection Law for Public Security and Criminal Investigation (Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal, 2019).

This initiative aims to establish guidelines and parameters for handling personal data in the context of public security and criminal prosecution activities. It strives for safeguarding the rights of data subjects against misuse and abuse while also providing authorities with access to the full potential of modern tools and platforms for public security and investigative purposes. The protection of people's fundamental rights to security, freedom, privacy, and the development of their own personality, and the guarantee of effective action towards these activities by responsible government agencies are part of the main objectives of this project, guaranteeing basic fundamentals for the protection of personal data in public security and criminal prosecution activities[130]. While it emphasizes that the processing of personal data for State security and national defense activities may be carried out provided there is a specific legal provision[131] (Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal, 2019).

Specifically, the proposed law addresses the critical aspects of surveillance technology and the processing of personal data within the context of public security. Chapter VII, entitled “Technologies for Monitoring and Treatment of Data High Risk” is therefore highly relevant to discussion of this work. In analysis, this chapter outlines stringent provisions for the use of

[130] Provided in art.1 and art.2.

[131] Provided in art. 7.

surveillance technologies and processing high-risk personal data by competent authorities. It mandates specific legal frameworks that must establish detailed usage policies, covering internal procedures, security measures, data access, retention policies, public access, shared usage scenarios, necessary training, and internal audits. Technical opinions, annual reports on nationwide surveillance technology usage, and audits in cases of non-compliance are required to be issued by the national authority. Besides, continuous, real-time surveillance in public security is restricted unless directly tied to individualized and lawfully authorized criminal prosecution (Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal, 2019).

This framework reinforces legal compliance, impact report transparency, and measures for safeguarding data subjects' rights through administrative and judicial oversight. Despite providing a comprehensive framework for the responsible and ethical utilization of surveillance technologies in public security, it is relevant to note that the proposed legislation has made no significant progress in the legislative process. Three years have passed since the Preliminary Draft Penal Data Protection Law was introduced, and yet, the proposal remains stagnant. Only one bill (Bill 1515/22), which incorporates certain segments of the preliminary draft, emerged in early June 2022. Regrettably, this development has led to the disappearance of Chapter VII from consideration (Projeto de Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais, 2022).

Undoubtedly, there is dissolution of the data protection system, posing risks to both rights and broader societal interests. As presented by Stefano Rodotà (2009), this setting of erosion of fundamental rights is associated with the security urgencies and state of exception[132].

[132] Both Stefano Rodotà (2009) and Solove (2021) identified 9/11 as turning point for the intensification of security concerns in opposition to privacy's rights. For instance, Rodotà (2009, p. 78) writes that "after 9/11 many reference criteria changed and the guarantees were reduced everywhere in the world". Moreover, Solove (2021, p.1-2) affirms that "especially after the terrorist attacks on September 11, 2001—the balance has shifted toward

Secondly, the inclination to reduce protective measures was expanded to areas seeking capitalization, particularly in business-related sectors. Lastly, the continual emergence of new technological possibilities[133] gives rise to a genuine technological drift that national and international authorities may not always effectively counteract (Rodotà, 2009).

This scenario poses risks to both rights and broader societal interests. Addressing these issues is essential to strike a balance between security needs and the data protection in an increasingly digital and surveillance-oriented society, which it was possible to notice with the Brazilian example. The mapping of technology usage and its progression over just a few years, where some states that initially did not utilize these technologies began doing so rapidly, make evident not only rapid evolution of technologies, but also its swift adoption by various public security agencies. This developmental tendency is not followed by a consistent legal apparatus in terms of protection.

> "We live at a time when the issues related to the protection of personal data feature a markedly contradictory approach – indeed, a veritable social, political and institutional schizophrenia. There is increased awareness of the importance of data protection as regards not only the protection of the private lives of individuals but their very freedom. This approach is reflected by many national and international documents, (...) where data protection is recognised as a fundamental, autonomous right. Still, it is increasingly difficult to respect this general assumption, because internal and international security requirements, market interests and the re-organisation of the public administration are heading towards the diminution of relevant safeguards, or pushing essential guarantees towards disappearance" (Rodotà, 2009, p. 77)

In contrast to the assurance of data protection, there is a consistent trend favoring the widespread adoption of technology in Brazil, also evidenced by legislative initiatives in the

the security side of the scale. The government has been gathering more information about people and engaging in more surveillance"

[133] As it will be seen in the following pages, "tools for classification, selection, social sorting and control of individuals" (Rodotà, 2009, p.78).

form of bills. This trend is exemplified by the work of the civil organization “Tire Meu Rosto da Sua Mira"[134], which has documented the increasing push for the exclusive utilization of technology in various regions. For instance, in the state of Minas Gerais, Bill 391/2019 has been proposed, advocating for the mandatory integration of facial recognition technology in public spaces under the jurisdiction of the state. Additionally, in Rio de Janeiro, Bill 318/2019 has been put forth, aiming to enforce the compulsory implementation of facial recognition technology across common areas, encompassing both public and private events with attendance exceeding ten thousand individuals within the state of Rio de Janeiro[135] (Tire Meu Rosto da Sua Mira, 2022).

Hence, an opposing trend is observed wherein the implementation of technologies is supported and incentivized, at times mandated by legal provisions, while there is a void of legal safeguards to protect data. While legislative frameworks exist, as previously highlighted, they fail to encompass the domain where data plays a pivotal role, particularly within the public security context, and especially considering surveillance technologies.

> "The privacy-security debate profoundly influences how these government activities are regulated. But there’s a major problem with the debate: Privacy often loses out to security when it shouldn’t. Security interests are readily understood, for life and limb are at stake, while privacy rights remain more abstract and vague" (Solove, 2021, p.2)

Consequently, this void creates a fertile ground for ethical dilemmas and potential challenges within the sector, as previously presented in this work. The concerns about the impact of technological advancements on public surveillance may escalate, especially in light of ongoing technological advancements endowed with capabilities for classification, selection,

[134] “Take my face out of your gunsight”.

[135] https://tiremeurostodasuamira.org.br/mapeamento/

social sorting, and control within the realm of public surveillance that often rely on technology to address social complexities (Rodotà, 2009).

In a sum, the journey through the intricate dimension of surveillance technologies and data protection reveals a delicate balance between the imperative of security and the safeguarding of fundamental rights. The cited perspective on the unrelenting process of reinventing data protection underscores its indispensability. It is not merely a legal necessity but a shield against the encroachment of societies into realms of "control, surveillance, and social selection" (Rodotà, 2009, p.82).

The reimagination of data protection emerges as an indispensable process, being crucial for averting the exacerbation of risks and vulnerabilities, especially emanating from entities deeply entrenched in surveillance and security measures. In line with Rodotà's (2009) perspective, the concept of reinventing data protection is akin to embracing a necessary utopia:

> "A utopia that does not direct our gaze towards the remote future but rather obliges us to consider the reality surrounding us. Data protection is not only a fundamental right among others but the most expressive of the contemporary human condition. Recalling this at all times is not vaniloquy, because any changes affecting data protection impact on the degree of democracy we all can experience." (Rodotà, 2009, p. 82)

The absence of a robust legal framework for data protection has far-reaching consequences also on the sociopolitical fabric. In the context of public security and surveillance, this underscores the critical role to ensure not only individual rights but also the broader democratic values, such as equality, that define societal dimension. This lackness raises significant concerns, particularly regarding its potential impact on vulnerable populations. For instance, examining sensitive data, such as racial information, becomes pivotal as it can exemplify biases both in data production and in shaping security policies. The failure to adequately protect sensitive data carries the risk of fostering discrimination, amplifying societal disparities, and compromising the principles of equality and justice.

Finally, the failure to adequately create a robust protective mechanism carries the risk of fostering discrimination, amplifying societal disparities, and compromising the principles of equality. Reenvisioning regulatory frameworks for data protection in the context of security policies is not just a procedural adjustment, but also an ethical imperative. It involves crafting legislation that not only addresses legal gaps but also actively works towards dismantling systemic biases, fostering transparency, and ensuring accountability.

In conclusion, the comprehensive exploration of the intersection between technology, security, and rights in the Brazilian context unveils a situation marked by ethical complexities and legal inadequacy. The intertwining of public and private entities in the acquisition and utilization of surveillance technologies raises concerns about transparency, accountability, and the potential erosion of democratic values. The deployment of advanced surveillance technologies in public security operations has not only transformed the dynamics of data collection and processing but has also given rise to critical challenges that demand urgent attention. The classification and processing of extensive datasets in surveillance technologies enable powerful capabilities in law enforcement. The impact of these technologies extends beyond technical considerations and intersects with broader societal issues, including racism. The discriminatory biases in data-driven technologies, particularly in the context of public security, reinforce pre-existing inequalities, and the failure to advance legislation creates legal ambiguities and potential for abuse. Ultimately, the protection of data becomes an instrument for achieving equality and freedom, transcending discrimination and deprivations.

Final Considerations

The engaging thematic of public security through surveillance technologies designated a multifaceted and interdisciplinary approach to identify, characterize and analyze contemporary society in terms of governance, politics, law and rights.

In the era of the Fourth Industrial Revolution, where technological advancements are intertwined with social fabric, the theme of surveillance technologies within the context of public security holds profound relevance (Schwab, 2016). The integration of cutting-edge technologies, such as artificial intelligence, data analytics, and interconnected systems, has ushered in unprecedented capabilities for surveillance.

This broader context is fundamental for the development of this research with the overarching goal of comprehensively investigating the intricate relationship of surveillance technologies and the public security sector. The formulation of research questions aimed at understanding the evolution of surveillance tools, their role in shaping power dynamics within governments, their specific influence on Brazil's security field, and the ethical and legal challenges associated with their deployment. To achieve these objectives, a qualitative methodology was adopted facilitating a nuanced exploration of the meanings, concepts, and characteristics associated with surveillance technologies and public security.

The exploratory nature of the research allowed for a comprehensive understanding of the multifaceted problem at hand. The study delved into existing literature, theories, and practical applications to identify key issues, and challenges related to surveillance technologies. This work delved into Michel Foucault's (1999) analysis in "Discipline and Punish: The Birth of the Prison". Understanding the evolution of techniques of power provides a profound lens through which it is possible to examine contemporary surveillance technologies. In today's sophisticated surveillance systems, characterized by constant monitoring, systematic codification, and data processing, Foucault's concept of disciplinary power finds a parallel. His exploration of disciplinary power, marked by meticulous control over the body's operations, resonates with the principles underpinning current surveillance modes. These systems not only control but actively generate knowledge about individuals based on societal norms, reflecting the normalizing judgment mechanism highlighted by Foucault (1999). The interdependence between power and knowledge, as articulated by the author, becomes particularly pertinent in the realm of surveillance technologies. The metaphor of the Panopticon, an architectural model designed for constant visibility and unverifiability, encapsulates the essence of contemporary surveillance technologies, not due to the format, but to the mechanism and process involved.

To stimulate understanding and contextualize theoretical perspectives, practical examples were employed. By identifying ongoing projects and plans involving surveillance technologies in Brazil's public security domain, the research has shed light on the specific influence these tools exert on the country's security landscape. The choice to focus in the country is justified by its geographical expanses, its substantial population, and the integration to the Global South susceptibility of testing emerging trends and widespread deployment of such technologies.

It was observed an incentive to the formulation and adoption of public security policies involving surveillance technologies, as with the Plano Nacional de Segurança Pública e Defesa Social 2021-2030 (Plano Nacional de Segurança Pública e Defesa Social 2021-2030, 2021). Once this plan was identified, justification for the utilization were concentrated in the cost-benefit analysis and the level of criminality in the country, marked by low-security rating and sheer volume of homicides, that places the country as one of the most dangerous in the world (UNDP, 2021; Institute for Economics and Peace, 2022; Fórum Brasileiro de Segurança Pública, 2022). These figures underscore the imperative for a nuanced equilibrium between public safety imperatives and the protection of individual rights, highlighting the potential pitfalls associated with an overreliance on technological solutions, often referred to as technosolutionism.

In fact, Brazil's security sector is experiencing a paradigm shift, and to understand that, this work executed an extensive collection of documents for mapping governmental entities, and categorizing technologies. Noteworthy is the prominence of these technologies in various Brazilian states, reflecting a nationwide trend with the widespread adoption of facial recognition, drones, body cameras, OCR, and predictive policing. After the identification of public policies that employ such technologies, it became crucial to analyze the implementation through a critical lens, considering challenges, error facts and limitations.

Addressing the complex challenges in public security involves navigating the intricate relationship between private technology corporations and law enforcement agencies. The intertwining of private technology corporations with public security operations raises concerns about the potential influence of profit motives on law enforcement practices, it poses risks of monopolies, and long-term dependence, and oversight of diverse community needs with standardized solutions may reinforce surveillance-oriented models, emphasizing the necessity for robust regulatory frameworks based on principles of transparency and accountability.

Concerning the limitations of the technology, errors, e.g in facial recognition, were identified due to inaccuracies in the software and the presence of biases, including historical, representational, and evaluative biases that have impact on individuals. These aspects can undermine the reliability of the application of this technology, increasing the risk of violating fundamental rights, particularly in terms of racial criteria. This is especially critical in a society like Brazil, where a significant portion of the population is comprised of black individuals, many of whom live in areas subjected to frequent law enforcement operations. The exposed scenario amplifies the impact of historical racial biases within an already marginalized environment, accentuating the urgency for ethical considerations in the deployment of such technologies.

In this manner, the study unveils a risk of encroaching on the freedom of racialized populations, given the racial bias in the algorithms. Arguments supporting the ban include criminal selectivity, the technology's lack of neutrality, indiscriminate public surveillance, and a social inversion of the presumption of innocence principle, as constant surveillance implies a presumption of guilt for everyone, or for some ones.

Faced with the potential for algorithmic errors and biases, the study undertook an analysis regarding the existence of specific legal regulations. The Brazilian General Law on Data Protection, enacted in August 2018, aimed to safeguard fundamental rights related to freedom, privacy, and personal data. However, the law excludes public security and criminal investigation, leaving a regulatory gap. This exclusion raises concerns about potential infringements on rights posed by the increasing use of technology in these domains. To address this gap, some efforts have been taken. Bills have been drafted and proposed, still the results were extremely limited, both due to the scope of protection and also to the little progress in the legislative process.

Therefore, the exploration of potential risks emanating from the use of surveillance technologies has underscored the intricate interplay between security imperatives and ethical considerations. Moreover, the absence of specific legal regulations accentuates the risks to fundamental rights of freedom, privacy, and personal data protection, underscoring the need for a comprehensive regulatory framework.

By fulfilling the research objectives, it has not only broadened the knowledge of the historical, ethical, and legal dimensions of surveillance technologies but has also emphasized the significance of a balanced and informed approach in deploying and regulating these tools. Still, it is important to acknowledge limitations in accessing official institutional data due to lack of systematic reporting and technical knowledge, confidentiality constraints, and the recent nature of public security policies.

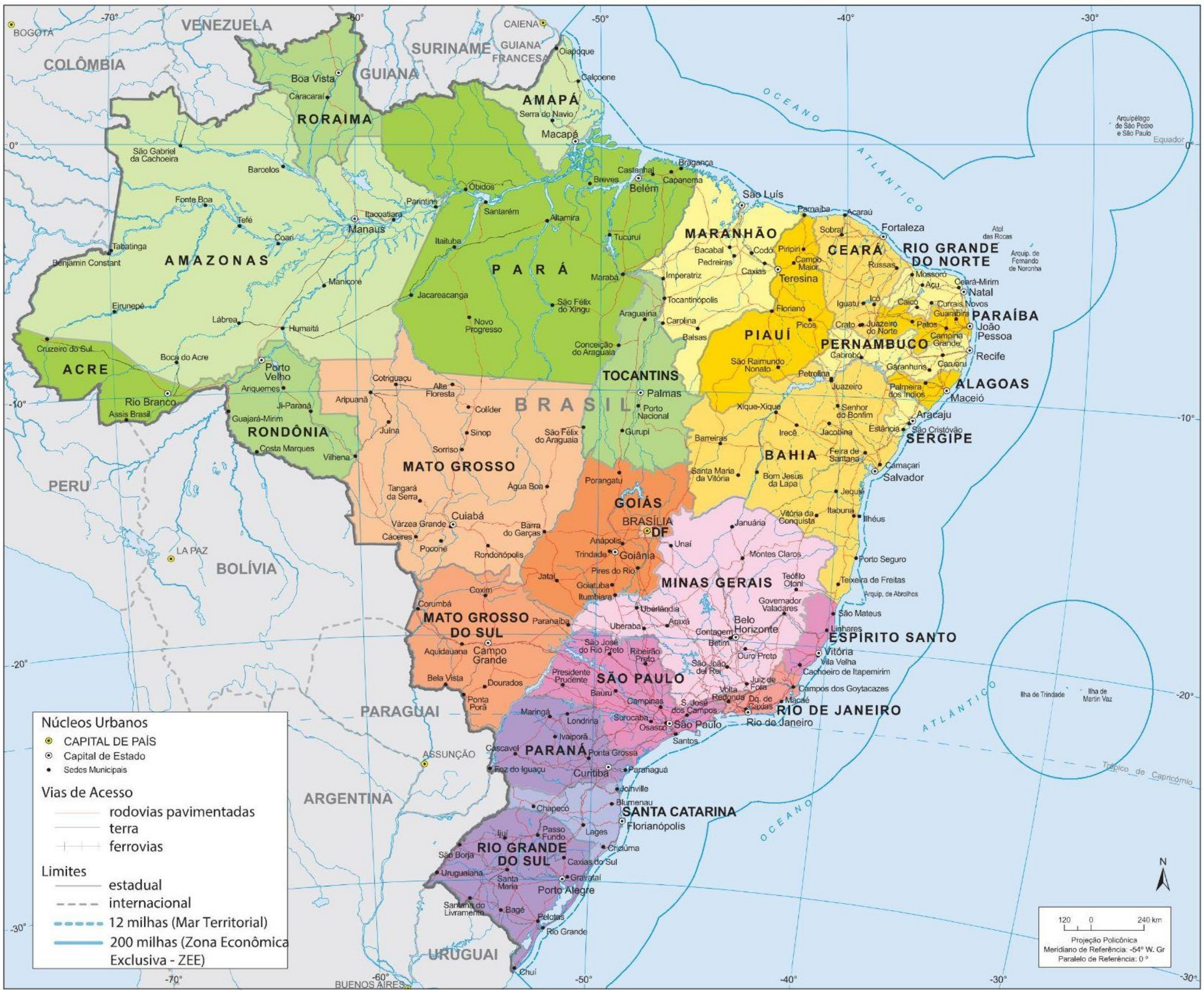
Ultimately, this research contributes to a nuanced comprehension of the multifaceted role played by surveillance tools in shaping power dynamics within public security, advocating for regulation efforts. In conclusion, the acknowledgment of contemporary conditions, specifically the rapid pace of technological change and its profound implications, reveals a common challenge faced by today's political, legislative, and regulatory authorities. There exists a duty to establish a shared set of values guiding policy decisions, it is imperative that the approach to creating, revising, and enforcing regulations evolves.

In light of the research findings, the complexity and sensitivity of the subject matter point towards promising avenues for further studies. This extends to various realms, encompassing public security policies, operational efficiency, innovation, and the protection of fundamental rights, including those related to freedom, privacy, and personal data. These considerations underscore the enduring importance of scholarly inquiry in shaping the discourse surrounding the interplay of surveillance tools, power dynamics, and regulatory frameworks in contemporary society.

Annexes

ANNEX A - MAP OF BRAZIL

This annex includes a map of Brazil, presented with the intention of enhancing the visualization of the areas where surveillance technologies are deployed for the public security sector.



Source: Instituto Brasileiro de Geografia e Estatísticas

Mapa do Brasil Político. (n.d.). IBGE. https://atlasescolar.ibge.gov.br/mapas-atlas/mapas-do-brasil/federacao-e-territorio

ANNEX B - POPULATION RANKING IN THE STATES OF BRAZIL

This annex offers a list of the ten most densely populated states in Brazil, aiming to offer a quantitative dimension to discussions surrounding data collection and processing. Once individuals generate data that are the input for systems that serve public security, it sheds light on the intricate challenge of safeguarding fundamental rights like freedom and privacy, potentially encountering biased policies in the process.

State	**Population**
São Paulo	44.420.459
Minas Gerais	20.538.718
Rio de Janeiro	16.054.524
Bahia	14.136.417
Paraná	11.443.208
Rio Grande do Sul	10.880.506
Pernambuco	9.058.155
Ceará	8.791.688
Pará	8.116.132
Santa Catarina	7.609.601

Source: Instituto Brasileiro de Geografia e Estatísticas

Instituto Brasileiro de Geografia e Estatísticas. (2022). Population Ranking In The States Of Brazil [Dataset]. In Censo 2022. IBGE. https://censo2022.ibge.gov.br/panorama/indicadores.html?localidade=BR

ANNEX C: CATEGORIZATION OF DATA

This annex provides a comprehensive overview of different data classifications provided by the Lei Geral de Proteção de Dados (2018) and the EU General Data Protection Regulation (2016), with examples to clarify the concepts of data in their different classification, facilitating readers' comprehension throughout the work.

Localization Data	Also known as geolocation data, localization data refers to information that pinpoints the physical location of an individual, device, or object on the Earth's surface. This includes data such as GPS coordinates and IP addresses.
Image data	Image data comprises visual information presented in the form of digital images or photographs. It is commonly employed in applications such as facial recognition.
Personal Data	It enables the direct or indirect identification of a natural person. For example, name and surname, date and place of birth, civic registration number, address, bank account, history of payment, IP address, etc.
Biometric Data	Biometric data results from specific technical

	processing related to the physical, physiological, or behavioral characteristics of an individual, enabling their unique identification. This category includes data such as facial images and fingerprints.
Sensitive Data	Those that reveal racial or ethnic origin, religious or philosophical convictions, political opinions, union membership, genetic, biometric issues and a person's health or sexual life.
Anonymized data	Originally related to a person, but which went through steps that ensured it was unlinked from that person.

Sources: Lei Geral de Proteção de Dados Pessoais, 2018; General Data Protection Regulation, 2016.

ANNEX D: BRAZILIAN GENERAL LAW ON DATA PROTECTION (LEI GERAL DE PROTEÇÃO DE DADOS - LGPD) - KEY PROVISIONS

This annex provides a summary of key provisions from the Brazilian General Law on Data Protection (Lei Geral de Proteção de Dados - LGPD)[136] that are relevant to the themes of data, surveillance, and public security. The LGPD, enacted regulation of the processing of personal data in Brazil, both in physical media and on digital platforms, as well as for public and private institutions, with the aim of protecting the fundamental rights of freedom and privacy and the free development of the personality of natural persons.

Fundamental ground	Art. 2 of the General Personal Data Protection Law - LGPD outlines the fundamental grounds: ● Respect for privacy ● Informative self-determination ● Freedom of expression, information, communication, and opinion ● Inviolability of intimacy, honor, and image ● Economic and technological development and innovation ● Free initiative, free competition, and consumer protection ● Human rights, free development of personality, dignity, and the exercise of citizenship by natural persons.

[136] The full text on the Brazilian General Law on Data Protection can be found on: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm

Principles	According to Art. 6 of the LGPD, personal data processing activities must adhere to good faith and several principles ● Purpose: Processing must align with legitimate, specific, explicit, and informed purposes to the data subject. ● Adequacy: Processing should be compatible with the informed purposes and the context. ● Necessity: Limit processing to the minimum necessary, covering pertinent data, and avoiding excess. ● Free Access: Ensure data subjects have easy and free access to information about the processing. ● Data Quality: Guarantee accuracy, clarity, relevance, and updating of data to fulfill its processing purpose. ● Transparency: Provide clear, precise, and easily accessible information to data subjects about processing. ● Security: Utilize technical and administrative measures to protect personal data from unauthorized access. ● Prevention: Adopt measures to prevent damage due to personal data processing. ● Non-discrimination: Prohibit processing for illicit or abusive discriminatory purposes. ● Accountability: Demonstrate the adoption of effective measures and compliance with personal data protection rules.
Data Processing	Article 7 delineates the scenarios for data processing, including obtaining consent, legal or regulatory obligations, public administration

	requirements for public policies, research organization studies, contract execution, rights exercise, life protection, health protection, legitimate interests, and credit protection. The processing of sensitive personal data may occur only in specific cases, as outlined in Art. 11, ensuring explicit consent or when essential for legal obligations, public policies, studies, rights exercise, life or health protection, or fraud prevention and security.
Rights	From art. 17 to 20 it is granted that the data subject rights such as easy access to information about data processing, including the purpose, controller identification, responsibilities of processing agents, and the subject's rights. The data subject can also request confirmation of processing existence, access to data, correction of incomplete or inaccurate data, and deletion of data processed with consent.
Control	Art. 5 mandates the appointment of a person responsible for data processing by the controller. This person acts as a communication channel between the controller, data subjects, and the National Data Protection Authority (ANPD), handling complaints, providing clarifications, and guiding employees on data protection practices.
Exception	Certain forms of data processing are excluded from LGPD application, such as those for journalistic, artistic, and academic purposes, as well as

	information related exclusively to public security, national defense, state security, and investigation and repression activities of criminal offenses.

Source: Lei Geral de Proteção de Dados Pessoais, 2018.

Bibliography

Alencar, I. (2023, September 1). Com mais de mil prisões na BA, sistema de reconhecimento facial é criticado por “racismo algorítmico”; inocente ficou preso por 26 dias. G1. https://g1.globo.com/ba/bahia/noticia/2023/09/01/com-mais-de-mil-prisoes-na-ba-sistema-de-reconhecimento-facial-e-criticado-por-racismo-algoritmico-inocente-ficou-preso-por-26-dias.ghtml

Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal (2019). https://www.conjur.com.br/dl/anteprojeto-lei-disciplina-protecao.pdf

Arcoverde, L. (2023, August 7). *Prefeitura de SP assina contrato para instalar sistema de reconhecimento facial e prevê 200 câmeras até outubro no Centro contra tráfico de drogas*. G1. https://g1.globo.com/sp/sao-paulo/noticia/2023/08/07/prefeitura-de-sp-assina-contrato-para-instalar-sistema-de-reconhecimento-facial-e-preve-200-cameras-ate-outubro-no-centro-contra-trafico-de-drogas.ghtml

Badin, L., & Viana, M. T. (2022). Dados, tecnocontrole, autoridade e subjetividade. In: *A Vida Política Das Tecnologias Digitais*, 7–24. Editora PUC Rio.

Berg, B. L., & Lune, H. (2017). *Qualitative research methods for the Social Sciences* (9th ed.). Pearson Education.

Bittencourt, R. (2023, August). Segurança Pública recebe mais de 2 mil pistolas semiautomáticas do Governo do Estado. https://www.amapa.gov.br/noticia/0708/seguranca-publica-recebe-mais-de-2-mil-pistolas-semiautomaticas-do-governo-do-estado

Bomfim, F. (2021, December 17). Programa da Polícia Civil identifica homem errado e inocente é preso. *R7.com*. https://noticias.r7.com/brasilia/programa-da-policia-civil-identifica-homem-errado-e-inocente-e-preso-17122021

Bordignon, G. B. (2020). Dispositivos de vigilância como tecnologias de controle no capitalismo de dados. *Revista De Morfologia Urbana*. https://doi.org/10.47235/rmu.v8i2.157

Branco, P. (2019). Smart Cities como dispositivos biopolíticos. VI Simpósio International LAVITS 2019, Salvador, Brazil. https://lavits.org/wp-content/uploads/2019/12/TeixeiraBlanco-LAVITISS-2019.pdf

Castells, M. (2010). Rise of the Network Society: The Information Age: Economy, Society and Culture. In *Blackwell Publishers Inc. eBooks* (2nd ed.). John Wiley & Sons, Ltd. https://deterritorialinvestigations.files.wordpress.com/2015/03/manuel_castells_the_rise_of_the_network_societybookfi-org.pdf

Constituição Da República Federativa Do Brasil. (1988). https://constituicao.stf.jus.br/dispositivo/cf-88-parte-1-titulo-5-capitulo-3-artigo-144

Da Silva, P. P. (2022). Racismo através do tecnicismo: dissecando a lógica racial da polícia preventiva. In: *Vida política das tecnologias digitais* (pp. 83–108). Editora PUC Rio.

De Laat, P. (2019). The disciplinary power of predictive algorithms: a Foucauldian perspective. *Ethics and Information Technology*, *21*(4), 319–329. https://doi.org/10.1007/s10676-019-09509-y

De Moraes, F. O. (2022). *Policiamento preditivo e aspectos constitucionais* [MA Thesis]. Pontifícia Universidade Católica do Rio de Janeiro.

Deleuze, Gilles. (1988). *Foucault*. University of Minnesota Press.

Deleuze, Gilles. (2013). Post-scriptum sobre as sociedades de controle. In: *Conversações*: 1972-1990. Editora 34. p. 223-230.

Dias, T., & Hvistendahl, M. (2021). Polícia do Rio comprou tecnologia da Oracle usada por países autoritários. *Intercept Brasil*. https://www.intercept.com.br/2021/03/10/policia-rio-tecnologia-oracle-policias-paises-autoritarios/

DIEESE. (2022). *BRASIL: A inserção da população negra no mercado de trabalho*. https://www.dieese.org.br/infografico/2022/populacaoNegra2022/index.html?page=4

Feldstein, S. (2019). The global expansion of AI surveillance. Carnegie Endowment for International Peace. https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

FGV Direito Rio. (2023). Segurança pública na era do Big data. https://direitorio.fgv.br/publicacao/seguranca-publica-na-era-do-big-data

Fleuri, R. M. (2008). Rebeldia e democracia na escola. Revista Brasileira De Educação, 13(39), 470–594. https://www.scielo.br/j/rbedu/a/JDbygKckc9y3g93ZgPqPZmK/?format=pdf&lang=pt Retrived 20 August 2023.

Fórum Brasileiro de Segurança Pública. (2022). Anuário Brasileiro de Segurança Pública. In Fórum Brasileiro De Segurança Pública.

Foucault, M. (1980). Nietzsche, Genealogy, History. In D. Bouchard (Ed.), *Language, Counter-Memory, Practice: Selected Essays and Interviews* (pp. 139-164). Ithaca, NY: Cornell University Press. https://doi.org/10.1515/9781501741913-008

Foucault, M. (1995). *Discipline and punish: The Birth of the Prison* (A. Sheridan, Trans.). Vintage Books. https://monoskop.org/images/4/43/Foucault_Michel_Discipline_and_Punish_The_Birth_of_the_Prison_1977_1995.pdf

Foucault, Michel (2010). *Em defesa sociedade: Curso no Collège de France (1975-1976)* (2nd ed.). Martins Fontes.

G1 Rio. (2019, November 7). Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano. G1. https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml

G1. (2022, January 7). *Foto de astro do cinema Michael B. Jordan aparece em lista de procurados pela polícia do Ceará*. https://g1.globo.com/ce/ceara/noticia/2022/01/07/astro-do-cinema-michael-b-jordan-aparece-em-lista-de-procurados-pela-policia-do-ceara.ghtml

General Data Protection Regulation. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. (2016, April 27). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504

Gil, A. C. (2002). *Como Elaborar Projetos de Pesquisa* (4th ed.). Editora Atlas. https://files.cercomp.ufg.br/weby/up/150/o/Anexo_C1_como_elaborar_projeto_de_pesquisa_-_antonio_carlos_gil.pdf

Governo do Estado da Bahia. (2023, August 1). Reconhecimento Facial tem média de dois foragidos localizados por dia em 2023. Portal Gov Bahia. https://www.bahia.ba.gov.br/2023/08/noticias/seguranca/reconhecimento-facial-tem-media-de-dois-foragidos-localizados-por-dia-em-2023/

Governo do Estado de São Paulo. (2017, May 15). Detecta monitora o Estado de SP com mais de três mil câmeras de vídeo. *Governo Do Estado De São Paulo*. https://www.saopaulo.sp.gov.br/spnoticias/detecta-monitora-o-estado-de-sao-paulo-com-3-mil-cameras-de-video/

Haggerty, K. D. (2006). Tear down the walls: on demolishing the panopticon. In *Theorizing Surveillance* (pp. 23–45). Willan Publishing. https://doi.org/10.4324/9781843926818-7

Han, B. (2018). *No enxame: Perspectivas do digital*. Editora Vozes Limitada. https://edisciplinas.usp.br/pluginfile.php/7574251/mod_resource/content/1/No%20enxame.pdf

Hardyns, W., & Rummens, A. (2017). Predictive policing as a new tool for law enforcement? Recent developments and challenges. *European Journal on Criminal Policy and Research*, *24*(3), 201–218. https://doi.org/10.1007/s10610-017-9361-2

Institute for Economics & Peace. (2022). Global Peace Index 2022: Measuring Peace in a Complex World. IEP. Retrieved September 2, 2023, from https://www.visionofhumanity.org/wp-content/uploads/2022/06/GPI-2022-web.pdf

Instituto de Defesa do Direito de Defesa - IDDD (2022). Pessoas negras têm 4 vezes mais chances de sofrerem abordagem policial . https://iddd.org.br/pessoas-negras-tem-4-vezes-mais-chances-de-sofrerem-abordagem-policial/

Instituto Igarapé. (2022). Metodologia para analisar a implementação de tecnologias de vigilância pelo Estado. In Instituto Igarapé. Retrieved September 1, 2023, from https://igarape.org.br/metodologia-para-analisar-a-implementacao-de-tecnologias-de-vigilancia-pelo-estado/

Instituto Igarapé. (2023). Implementação de tecnologias de vigilância no Brasil e na América Latina. In: Instituto Igarapé. Retrieved September 1, 2023, from https://igarape.org.br/implementacao-de-tecnologias-de-vigilancia-no-brasil-e-na-america-latina/

intelligence. (2023). In: *Cambridge Dictionary*. Retrieved August 19, 2023, from https://dictionary.cambridge.org/it/dizionario/inglese/intelligence

Johnson, J. (2019). Artificial intelligence & future warfare: implications for international security. *Defense & Security Analysis*, *35*(2), 147–169. https://doi.org/10.1080/14751798.2019.1600800

Kitchin, R. (2014). *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*. https://doi.org/10.4135/9781473909472

Lei 13.675. (2018, June 11). https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13675.htm

Lei Geral de Proteção de Dados Pessoais. Lei nº 13.709 (2018). https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Magaloni, B., Melo, V. P., & Robles, G. (2022). Warriors and Vigilantes as Police Officers: Evidence from a Field Experiment with Body-Cameras in Rio de Janeiro. Social Science Research Network. https://doi.org/10.2139/ssrn.4005710

Matzner, T. (2017). Opening Black Boxes Is Not Enough – Data-based Surveillance In Discipline and Punish And Today. *Foucault Studies*, 27–45. https://doi.org/10.22439/fs.v0i0.5340

Mello, D. (2023, August 31). Reconhecimento facial está presente em todos os estados do Brasil. *Agência Brasil*. https://agenciabrasil.ebc.com.br/geral/noticia/2023-08/reconhecimento-facial-esta-presente-em-todos-os-estados-do-brasil

Melo, P. V. (2021). A serviço do punitivismo, do policiamento preditivo e do racismo estrutural. Le Monde Diplomatique. https://diplomatique.org.br/a-servico-do-punitivismo-do-policiamento-preditivo-e-do-racismo-estrutural/

Moraes, F. D. O. (2022). *Policiamento Preditivo e Elementos Constitucionais* [MA thesis, Pontifícia Universidade Católica do Rio de Janeiro]. https://www.maxwell.vrac.puc-rio.br/59303/59303.PDF

Morais, C. (2022, October). Estado Forte, Povo Seguro: Governo do Amapá ativa patrulhamento aéreo de segurança com drones. Governo Do Estado Do Amapá. https://www.portal.ap.gov.br/noticia/1010/estado-forte-povo-seguro-governo-do-amapa-ativa-patrulhamento-aereo-de-seguranca-com-drones

Nunes, P. (2019). Exclusivo: levantamento revela que 90,5% dos presos por monitoramento facial no Brasil são negros. *Intercept Brasil*. https://www.intercept.com.br/2019/11/21/presos-monitoramento-facial-brasil-negros/

O'Neil, C. (2016). *Weapons of math destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown.

Perry, W. L. M., McInnis, B., Price, C. C., Smith, S., & Hollywood, J. S. (2013). *Predictive Policing: The role of crime forecasting in law enforcement operations. RAND Corporation*. https://doi.org/10.7249/rr233

Plano Nacional de Segurança Pública e Defesa Social 2021-2030. (2021). https://www.gov.br/mj/pt-br/centrais-de-conteudo/publicacoes/categorias-de-publicacoes/planos/plano_nac-_de_seguranca_publica_e_def-_soc-_2021___2030.pdf/view

Polícia Civil do Maranhão. (2023, June). Drones Serão Usados em Operações Da Polícia Civil do Maranhão. Polícia Civil do Maranhão. https://www.policiacivil.ma.gov.br/drones-serao-usados-em-operacoes-da-policia-civil-do-maranhao/

Presidência da República. (2021, April 30). Classificação dos Dados. Ministério Do Desenvolvimento E Assistência Social, Família E Combate À Fome. https://www.gov.br/mds/pt-br/acesso-a-informacao/lgpd/classificacao-dos-dados

Projeto de Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. PL n.1515. (2022) https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2182274

Rabinow, P. (2002). *Antropologia da Razão: Ensaios de Paul Rabinow*. Relume Dumará. (Original work published 1999)

Reis, C., Almeida, E., Dourado, F., & Silva, F. (2021). Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil. In LAPIN. Laboratório de Políticas Públicas e Internet.

Rodotà, S. (2009). Data protection as a fundamental right. In S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, & S. Nouwt (Eds.), *Reinventing Data Protection?* (pp. 77–82). Springer Netherlands. https://doi.org/10.1007/978-1-4020-9498-9_3

Rodrigues, G. D. S. (2022). Segurança Pública Datificada E Policiamento Preditivo [B.A Dissertation]. Universidade Federal do Rio de Janeiro.

Russell, S., & Norvig, P. (2010). *Artificial intelligence: A Modern Approach* (3rd ed.). Prentice Hall. https://people.engr.tamu.edu/guni/csce421/files/AI_Russell_Norvig.pdf

Saavedra, A. (2021, September 1). *Com câmeras de reconhecimento, Segup otimiza atuação e retira criminosos de circulação*. Agência Pará De Notícias. https://www.agenciapara.com.br/noticia/31086/com-cameras-de-reconhecimento-segup-otimiza-atuacao-e-retira-criminosos-de-circulacao

Schwab, K. (2016). *Fourth Industrial Revolution*. World Economic Forum. https://law.unimelb.edu.au/__data/assets/pdf_file/0005/3385454/Schwab-The_Fourth_Industrial_Revolution_Klaus_S.pdf

Secretaria da Segurança Pública e Defesa Social. (2021). SSPDS lança ferramenta Status para identificação de manchas criminais e tomadas de decisão. *Secretaria Da Segurança Pública E Defesa Social*. https://www.sspds.ce.gov.br/2021/02/04/sspds-lanca-ferramenta-status-para-identificacao-de-manchas-criminais-e-tomadas-de-decisao/

Secretaria de Administração Penitenciária. (2023, April). Seap adquire equipamentos de Sistema de Monitoramento. https://www.seap.am.gov.br/seap-adquire-equipamentos-de-sistema-de-monitoramentoos-materiais-serao-instalados-na-sede-administrativa-da-secretaria-e-nas-unidades-prisionais-da-capital/

Secretaria de Segurança Pública do Estado do Amazonas. (2020). PM do Amazonas desenvolve tecnologia de reconhecimento facial. SSP. Retrieved September 7, 2023, from https://www.ssp.am.gov.br/pm-do-amazonas-desenvolve-tecnologia-de-reconhecimento-facial/

Secretaria de Segurança Pública do Governo do Estado de São Paulo. (2017). *CARTILHA DE ADESÃO AO SISTEMA DETECTA – V3.0* [Slide show]. http://www.sapp.org.br/sapp/wp-content/uploads/Sistema_Detecta_cartilha_completa_v3.pdf

Selbst, A. D. (2017). Disparate impact in big data policing. *Social Science Research Network*. https://doi.org/10.2139/ssrn.2819182

Solove, D. J. (2011). *Nothing to hide: the false tradeoff between privacy and security* (Vol. 49). Yale University Press.

Tire Meu Rosto Da Sua Mira. (2022, August 16). *Mapeamento - #TireMeuRostoDaSuaMira*. https://tiremeurostodasuamira.org.br/mapeamento/

United Nations Conference on Trade and Development. (2023). Data protection and privacy legislation worldwide. UNCTAD. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

United Nations Development Programme. (2021). Independent Country Programme Evaluation: Brazil. In UNDP. UNDP Independent Evaluation Office.

Velasco, C., Croquer, G., & Pinhoni, M. (2023, August 29). *Monitor da Violência: PMs de 7 estados usam câmeras corporais; outros 10 estados dizem que a adoção está em andamento*. G1. https://g1.globo.com/monitor-da-violencia/noticia/2023/08/29/monitor-da-violencia-pms-de-7-estados-usam-cameras-corporais-outros-10-estados-dizem-estar-fazendo-testes-ou-avaliando-uso.ghtml

Verus, I. (2022, December 23). Estado e Prefeitura de Rio Branco firmam acordo para uso de 365 câmeras na capital - Noticias do Acre. Noticias Do Acre. https://agencia.ac.gov.br/estado-e-prefeitura-de-rio-branco-firmam-acordo-para-uso-de-365-cameras-na-capital/

Webster, F. (2006). *Theories of the Information Society* (3rd ed.). Routledge. https://cryptome.org/2013/01/aaron-swartz/Information-Society-Theories.pdf

Werthein, J. (2000). A sociedade da informação e seus desafios. *Ciência Da Informação*, *29*(2), 71–77. https://doi.org/10.1590/s0100-19652000000200009

Zuboff, S. (2015). Big other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, 30(1), 75–89. https://doi.org/10.1057/jit.2015.5

Zuboff, S. (2019). *The age of surveillance capitalism: The Fight for a Human Future at the New Frontier of Power*. Public Affairs.