

FROM SURVEILLANCE CAPITALISM TO DEMOCRATIC REGULATION: LEGAL AND ETHICAL CHALLENGES IN THE AGE OF DATA

DO CAPITALISMO DE VIGILÂNCIA À REGULAÇÃO DEMOCRÁTICA: DESAFIOS JURÍDICOS E ÉTICOS NA ERA DOS DADOS

DOI: 10.19135/revista.consinter.00021.12

Recebido/Received 26/05/2025 – Aprovado/Approved 07/08/2025

Anderson Filipini Ribeiro¹ – <https://orcid.org/0009-0008-5145-2476>

Filipe de Mello Sampaio Cunha² – <https://orcid.org/0009-0005-7142-8885>

Natalia Maria Ventura da Silva Alfaya³ – <https://orcid.org/0000-0002-0312-3677>

Abstract

The digital age has intensified the use of monitoring technologies and the massive collection of personal data, shaping the so-called surveillance society. This phenomenon, led by states and corporations, challenges the protection of fundamental

¹ PhD student in Law; Master in Law; Bachelor in Law and Theology; Specialization in Law, Internet and Society, Civil and Procedural Law, Labor Law, Criminal Law, and Military Law. Language skills at B1 level in Spanish (DELE), French (DELF), and Italian (CILS). Lattes: <http://lattes.cnpq.br/0703783803020290>. Email: direito.andersonfilipini@gmail.com. <https://orcid.org/0009-0008-5145-2476>

² Master in Law from Faculdades Londrina, he has a degree in Political Science from the University of Brasília and in Law from Centro Universitário Processus, with specializations in Public Management, BPM-CBOK Process Management, as well as Water Management and Sustainability of Water Resources in Brazil. Former Director of the National Water and Basic Sanitation Agency (ANA). President of the Institute of Regulation, Innovation, and Sustainability (IRIS). Lattes: <http://lattes.cnpq.br/4680398321828617>. Email: filipemgm@gmail.com. <https://orcid.org/0009-0005-7142-8885>

³ PhD in Legal and Social Sciences. Master's in Business Law. Law graduate. Lawyer. Lecturer. Researcher with the group Democracy, Citizenship and the Rule of Law - DeCIED and with the Gilvan Hansen Institute - IGH. Focusing especially on Democracy and democratic participation, Latin American constitutionalism, and peripheral modernity, with main theoretical bases in Jürgen Habermas and Jessé Souza. Email: naty.alfaya@gmail.com. Lattes: <http://lattes.cnpq.br/9731930696524695>. <https://orcid.org/0000-0002-0312-3677>

The linguistic revision of this manuscript and the translation from Portuguese to English were carried out by Paola Filipini Ribeiro.

We declare, for all due purposes, that during the preparation of this article I used the Artificial Intelligence tool specified below, with the aim of improving the clarity, cohesion and linguistic quality of the manuscript. All content generated by this technology was carefully reviewed and edited by me, assuming full responsibility for the accuracy, integrity and reliability of the information presented.

rights, especially privacy, freedom, and informational self-determination. Initially justified by security needs, digital surveillance has become a structural element of social, economic, and political relations, requiring reflection on its ethical and legal boundaries. The central problem of this study is reconciling the use of surveillance technologies with the preservation of fundamental rights. Two hypotheses are proposed: (i) the absence of robust regulations and effective social control mechanisms favors abusive and disproportionate practices; (ii) it is possible to harmonize technological innovation and the protection of fundamental rights through a democratic, transparent, and ethically oriented regulatory framework. The general objective is to analyze the impacts of digital surveillance on fundamental rights, emphasizing the regulatory duties of the state and companies. The specific objectives include discussing the risks of indiscriminate data collection, assessing the effectiveness of existing legislation, and proposing pathways for an ethical and democratic digital governance. The methodology consists of a qualitative bibliographic review based on legal doctrine, legislation, and technical reports. The study concludes that mass surveillance imposes unprecedented challenges to democracy, requiring the strengthening of digital citizenship, regulatory improvement, and public policies that reconcile innovation, rights protection, and informational justice.

Keywords: Digital surveillance; Privacy; Data protection; Fundamental rights; Digital governance.

Resumo

A era digital intensificou o uso de tecnologias de monitoramento e a coleta massiva de dados pessoais, configurando a chamada sociedade da vigilância. Esse fenômeno, protagonizado por Estados e corporações, desafia a proteção de direitos fundamentais, especialmente a privacidade, a liberdade e a autodeterminação informativa. A vigilância digital, inicialmente justificada pela segurança, tornou-se estruturante nas relações sociais, econômicas e políticas, impondo reflexão sobre seus limites éticos e jurídicos. O problema central deste estudo é compatibilizar o uso de tecnologias de vigilância com a preservação dos direitos fundamentais. Formulam-se duas hipóteses: (i) a ausência de regulamentações robustas e mecanismos de controle social favorece práticas abusivas e desproporcionais; (ii) é possível harmonizar inovação tecnológica e proteção de direitos fundamentais por meio de arcabouço normativo democrático, transparente e eticamente orientado. O objetivo geral é analisar os impactos da vigilância digital sobre direitos fundamentais, enfatizando deveres regulatórios de Estado e empresas. Os objetivos específicos incluem discutir riscos da coleta indiscriminada de dados, avaliar a efetividade das legislações e propor caminhos para uma governança digital ética e democrática. A metodologia consiste em revisão bibliográfica qualitativa com base em doutrina, legislação e relatórios técnicos. Conclui-se que a vigilância em massa impõe desafios inéditos à democracia, exigindo fortalecimento da cidadania digital, aprimoramento regulatório e políticas públicas que conciliem inovação, proteção de direitos e justiça informacional.

Palavras-chave: Vigilância digital; Privacidade; Proteção de dados; Direitos fundamentais; Governança digital.

Summary: 1. Introduction; 2. Contemporary Perspectives on Surveillance and Law; 3. The Role of the State in the Surveillance Society; 4. The Role of Companies and Private Surveillance; 5. Impacts of the Vigilância sobre Direitos Fundamentais; 6. Challenges and Perspectives for the Future; 7. Final Considerations; 8. References.

1 INTRODUCTION

Contemporary society is undergoing a profound transformation resulting from the exponential advancement of digital technologies and the broad connectivity provided by the internet, mobile networks, and cloud data infrastructures. Such innovations have been reshaping the forms of production, communication, consumption, and governance, while simultaneously enabling a degree of monitoring and social control unprecedented in human history. This structural reconfiguration, often invisible to the eyes of ordinary citizens, is one of the most striking features of what scholars such as Shoshana Zuboff call "surveillance capitalism" - an economic model based on the capture, processing, and commercialization of individuals' personal data as raw material for predicting and modulating behavior.

This is not merely a technical phenomenon, but a political, legal, and ethical reconfiguration of the very foundations of social life. The digitalization of social and administrative processes, combined with the power of massive data analysis, has allowed governments and companies to collect sensitive information in real time, often without due consent or control by data subjects. This scenario challenges traditional models of privacy protection, demanding a reinterpretation of fundamental rights in light of new technological paradigms. Surveillance, once associated with punitive mechanisms or national security, now extends to the daily activities of individuals: consumption habits, ideological preferences, urban movements, social interactions, and even biometric and genetic data.

Contemporary literature on the subject has pointed to a growing erosion of spaces of anonymity, intimacy, and informational self-determination. As Stefano Rodotà warns, privacy in the digital age has ceased to be a luxury or a reserved sphere and has become a condition for the possibility of human freedom and dignity. In other words, ubiquitous surveillance - operated by sensors, cameras, algorithms, and artificial intelligence - redefines the boundaries between the public and the private, making a profound debate on the ethical and legal limits of state and corporate action in cyberspace imperative.

In this context, the relevance of the present study is evident from both a scientific and social perspective. From a legal standpoint, the surveillance society challenges the pillars of contemporary constitutionalism, especially regarding the protection of the private sphere, equality of treatment, and due process of law. The massive collection of data can lead to algorithmic discrimination, mass control, and the suppression of civil liberties, eroding the foundations of the Democratic Rule of Law. From a social perspective, there is a clear power imbalance between citizens and the entities that possess the technical and economic capacity to process large volumes of personal information, thereby increasing the vulnerability of already marginalized populations and hindering the realization of social justice.

The central problem guiding this investigation therefore lies in the tension between individual rights and institutional duties in a hyperconnected society, in which surveillance has ceased to be an exception and has become a structural logic.

How can it be ensured, in this new paradigm, that technological advances are not used for authoritarian, discriminatory, or commercial purposes that violate individual autonomy? How can the need for public security be balanced with respect for fundamental guarantees? What are the ethical, legal, and democratic limits of large-scale surveillance?

Starting from the identified central problem, two main hypotheses are formulated that guide this investigation. The first hypothesis holds that, in the absence of robust regulations and effective mechanisms of social control, the advancement of surveillance technologies tends to produce a structural imbalance between the protection of privacy and the demands of security, favoring practices of mass data collection that violate fundamental rights. This hypothesis presupposes that the insufficiency of legal and institutional safeguards not only weakens informational self-determination but also increases the risks of algorithmic discrimination and abusive surveillance by state and private actors.

The second hypothesis is based on the premise that it is possible to reconcile technological innovation and the protection of fundamental rights through the adoption of a democratic, transparent regulatory framework grounded in clear ethical principles. From this perspective, legislation such as the Brazilian LGPD and the European GDPR offer relevant insights, but still lack practical effectiveness given algorithmic opacity and the transnational nature of data flows. This hypothesis considers that the consistent application of these frameworks, combined with mechanisms of auditing, social participation, and accountability, could mitigate the inherent risks of the surveillance society and promote a more balanced, fair digital environment that respects human dignity.

Thus, the investigation proceeds from the understanding that the empirical and theoretical testing of these hypotheses will allow the identification of whether the current normative and institutional arrangement is capable of adequately responding to the challenges posed by digital surveillance. By articulating the diagnosis of regulatory weaknesses with a comparative analysis of international experiences, the aim is not only to confirm or refute the hypotheses, but also to offer concrete inputs for the improvement of public policies and business practices in the processing of personal data. In this way, the research intends to contribute to the delineation of a digital governance model that ensures the effectiveness of fundamental rights, harmonizing innovation, security, and informational justice.

The justification of the study rests on the urgent need to understand and regulate the surveillance mechanisms that shape social and institutional life in the digital age. Although there have been relevant normative advances, such as the enactment of the Brazilian General Data Protection Law (Lei nº 13.709/2018) and the European Union's General Data Protection Regulation (GDPR), a significant gap remains between formal legislation and the effective monitoring practices carried out by both public bodies and private digital platforms. The increasing sophistication of artificial intelligence systems and the opacity of algorithms aggravate this challenge, as many automated decisions that directly affect citizens' lives - such as

credit approval, job offers, security screening, and access to public policies - occur without transparency, accountability, or the possibility of contestation.

Thus, the general objective of this article is to analyze the impacts of digital surveillance on fundamental rights, in light of the actions of the State and companies in the processing and control of personal data. More specifically, it aims to: (i) understand the legal risks and challenges related to the collection and mass processing of data; (ii) examine the implications of surveillance for privacy, freedom, equality, and dignity of individuals; (iii) evaluate the role of the State in regulating and overseeing these practices; and (iv) propose paths for strengthening an ethical, democratic digital governance aimed at the protection of human rights.

The methodology adopted is a qualitative bibliographic review, with an interdisciplinary focus, incorporating references from the fields of Law, Political Science, Sociology, and Philosophy. Classic and contemporary works by authors such as Ferdinand Lassalle, Stefano Rodotà, Shoshana Zuboff, Holmes and Sunstein, among others, are examined, as well as national and international normative documents, technical opinions, and research reports on data protection, digital surveillance, and fundamental rights. The method enables a critical analysis of surveillance practices, observing their concrete effects on citizenship and the legal system, with a view to formulating regulatory proposals appropriate to the current context.

The structure of the article is divided into six parts, in addition to the introduction and final considerations. The second chapter presents the theoretical and doctrinal perspectives on the phenomenon of digital surveillance, contextualizing its origins, foundations, and implications. The third chapter discusses the role of the State, its constitutional responsibilities, and the tensions between security and freedom. The fourth chapter analyzes the actions of private companies and the challenge of reconciling data-driven business models with the protection of fundamental rights. The fifth chapter addresses the concrete impacts of surveillance on personality rights, with emphasis on privacy, the right to be forgotten, and algorithmic discrimination. The sixth chapter examines the challenges and perspectives for the future, proposing normative, ethical, and institutional alternatives for a digital governance that respects democratic principles.

In summary, this study aims to contribute to the academic and institutional debate on the limits and possibilities of digital surveillance in a pluralistic, democratic society committed to the promotion of human rights. Critical reflection on existing normative instruments, the risks of unregulated technological control, and strategies for building an active digital citizenship constitute the main contributions of the research. In a world increasingly driven by data, algorithms, and digital platforms, ensuring freedom, transparency, and informational justice is a collective and urgent task - a task that demands not only laws, but also critical awareness, institutional responsibility, and social participation.

2 CONTEMPORARY PERSPECTIVES ON SURVEILLANCE AND LAW

Contemporary society is marked by an intense debate on digital surveillance and its impacts on fundamental rights. To understand this phenomenon at the intersection of constitution, privacy, freedom, and state regulation, Lassalle argues that the Constitution is not a mere set of legal norms, but rather the expression of the dominant social forces at a given time. Thus, in the context of digital surveillance, the Constitution must reflect the challenges imposed by technology on the balance between security and privacy (Lassalle, 1998).

Discussing digital surveillance, Rodotà reinforces the idea that privacy is an essential right in the information age. For him, mass surveillance carried out by States and companies represents a significant risk to individual autonomy. In this sense, privacy cannot be seen merely as an individual right, but as a fundamental pillar for the maintenance of democracy and human dignity (Rodotà, 2008).

The relationship between freedom, security, and state regulation, according to Holmes and Sunstein, cannot exist without a structure to sustain it, requiring effective regulation to balance the interests of the State and citizens. In this context, digital surveillance may be justified under the pretext of public security, but without adequate control mechanisms, it can lead to the suppression of fundamental rights (Holmes; Sunstein, 2019).

Zuboff, in turn, introduces the concept of surveillance capitalism, highlighting the role of large corporations in data monitoring. According to the author, technology companies capture personal information to predict and influence individuals' behavior, creating an economy based on the extraction and commercialization of data. This model, besides compromising privacy, also redefines power relations in contemporary society (Zuboff, 2021).

According to Corrêa and Fagundes Filho, net neutrality and the protection of personal data are central themes in the surveillance society. The absence of efficient regulation may result in the unbridled exploitation of users' information by companies operating in unregulated digital markets (Corrêa; Fagundes Filho, 2022).

Silva emphasizes that the positivization of data protection as a fundamental right is an urgent necessity in the era of surveillance capitalism. The author argues that the manipulation of personal information without explicit consent compromises individuals' informational self-determination, requiring a legal approach that ensures greater control over one's own data (Silva, 2021).

Technological advancement strengthens the State's empowerment in surveillance practices. Figueiredo et al. argue that the collection and processing of personal data become instruments of social control, challenging the constitutional principles of privacy and data protection. The expansion of these practices without adequate regulation can generate scenarios of abuse and discrimination (Figueiredo et al., 2021).

The historical perspective also aids in understanding this phenomenon, considering that according to Monteagudo (2021), contemporary democracy faces unprecedented challenges in the face of ubiquitous surveillance, which compromises

transparency and trust in institutions. The author emphasizes the need for public policies that limit the invasion of privacy in the name of national security (Monteagudo, 2021).

Martin (2024) discusses digital abandonment and the need for a duty of parental surveillance on the internet. The absence of supervision can expose children and adolescents to risks, making it essential to develop adequate protection mechanisms for this vulnerable population.

Regarding the regulation of algorithms, Verbicaro (2022) points out the challenges of establishing clear parameters for the use of automated systems, especially with regard to transparency and accountability of algorithmic decisions, which can perpetuate inequalities and violate fundamental rights.

Thus, the limits of surveillance must be clearly defined so that monitoring does not become an irreversible threat to individual freedoms, requiring a balance between technological innovation and respect for fundamental rights, preventing democracy from being eroded by abusive monitoring practices (Monteagudo, 2021).

3 THE ROLE OF THE STATE IN THE SURVEILLANCE SOCIETY

The protection of privacy and personal data has become a fundamental responsibility of the State in the era of the surveillance society. Alberti (2022, p. 116) highlights that:

Mass surveillance has been justified as a mechanism of public security, but it frequently conflicts with fundamental guarantees, such as privacy and data protection. In this context, it is up to the State to balance these interests, ensuring that the collection and use of personal information does not exceed the limits imposed by human rights.

In the normative landscape, various regulations have been implemented to establish limits on the collection and processing of personal data by both public agencies and private companies. In Brazil, the *Lei Geral de Proteção de Dados* (LGPD - Law No. 13,709/2018) represents an important milestone, establishing principles such as purpose, adequacy, necessity, transparency, and non-discrimination. Similarly, in the European context, the *General Data Protection Regulation* (GDPR) sets a high standard for the protection of personal data, influencing legislation in several countries.

As the literature points out, these regulations face significant implementation challenges. The LGPD, although modern and aligned with international standards, still suffers from a lack of structure in inspection bodies and the absence of a consolidated digital culture that prioritizes the protection of informational privacy. The difficulty of applying effective sanctions to violators, especially large technology corporations operating globally, also constitutes a relevant obstacle to the effectiveness of the regulatory framework.

Rodotà (2008) argues that privacy has become an essential right, especially in a scenario where governments and corporations accumulate gigantic volumes of

personal information. In this respect, state action must therefore prioritize the guarantee of this right, promoting a balance between technological innovation and the protection of human dignity.

With regard to the relationship between freedom, security, and state regulation, according to Holmes and Sunstein (2019), freedom depends directly on the State's capacity to provide protection and security mechanisms. Thus, the regulation of surveillance must be accompanied by measures that ensure transparency and social control over the use of collected information.

Surveillance capitalism, a concept widely discussed by Zuboff (2021), reinforces the role of the State in regulating large technology corporations that, by capturing and commercializing personal data, challenge state regulatory power and impose new challenges to the protection of privacy and citizens' informational self-determination.

The applicability of disruptive technologies, such as facial recognition, in public surveillance systems in Brazil raises questions about their compatibility with the constitutional right to privacy. Silva (2022) analyzes how the absence of specific regulation can result in abuses and violations of fundamental rights.

The issue of the right to be forgotten also fits into this debate. In this regard, Siqueira et al. (2023) examine the (in)applicability of this right in the Brazilian legal system, evidencing the need for protection against the perpetuity of harmful information on the internet, with the State being responsible for establishing clear guidelines to balance the right to information and the protection of individual reputation.

Souza and Lima (2021) discuss how, in the information society, consent plays a central role in the protection of personal data. However, in the context of digital surveillance, consent is often obtained in a vague and non-transparent manner, making it difficult for individuals to exercise effective control over their information. The State must therefore act to ensure that consent is truly free, informed, and unequivocal, as provided for in legislation.

The regulation of algorithms, as highlighted by Verbicaro (2022), represents one of the greatest challenges in the protection of privacy. The growing use of artificial intelligence in governmental decision-making requires a normative framework that prevents discriminatory practices and ensures transparency in the use of these systems.

Thus, state action in the surveillance society must prioritize the protection of fundamental rights, ensuring that the pursuit of security does not become an instrument of excessive control. The adoption of public policies that promote transparency, informed consent, and rigorous oversight of the use of surveillance technologies is essential for the preservation of individual freedoms in the digital age.

4 THE ROLE OF COMPANIES AND PRIVATE SURVEILLANCE

The mass collection of data by technology companies has become one of the main characteristics of the information society. These corporations act as intermediaries in the flow of data, collecting personal information from different sources, such as social networks, applications, and connected devices. According to Zuboff (2021), this dynamic configures the so-called "surveillance capitalism," in which user data is transformed into a commodity for commercial purposes and behavioral predictability.

User consent, although a fundamental principle in data protection, is often presented in a questionable manner. As highlighted by Canavez, Santos, and Mendes (2022), privacy policies frequently use complex and inaccessible language, leading users to grant permissions without fully understanding the implications of their actions. This scenario raises the debate on the real validity of consent in the context of private surveillance.

According to Verbicaro (2021), the regulation of the use of algorithms is one of the main challenges of the Brazilian Internet Civil Rights Framework (*Marco Civil da Internet*), as it directly affects the fundamental rights of citizens. Thus, the lack of clarity in algorithmic processes compromises individual autonomy and increases the risks of discrimination and digital manipulation.

Corporate responsibility in the digital age has become a central issue in debates on data protection and fundamental rights. As pointed out by Souza and Lima (2021), companies need to adopt effective data governance measures, ensuring that collected information is used ethically and in compliance with current legislation. This includes the implementation of auditing and compliance mechanisms to prevent abuses.

The Brazilian General Data Protection Law (LGPD) and the European General Data Protection Regulation (GDPR) are regulatory frameworks that establish guidelines for the collection and processing of personal data. In this context, according to Corrêa and Fagundes Filho (2022), net neutrality and information security are essential aspects to ensure user privacy in the face of the advancement of digital surveillance.

The massive collection of data by private companies also has significant impacts on public security and the protection of individual rights. Monteagudo (2021) highlights that the use of surveillance technologies by corporations can result in the restriction of freedoms and excessive monitoring, creating an environment conducive to violations of fundamental rights.

Disruptive technologies, such as facial recognition, are also a topic of concern in the debate on privacy and digital security, as according to Silva (2022), these systems have been widely used by companies and the State, often without transparency or adequate control, raising questions about the effectiveness of constitutional rights to privacy.

The application of sanctions and penalties is a necessary measure to ensure that companies fulfill their obligations regarding data protection. According to

Siqueira et al. (2023), the discussion on the right to be forgotten exemplifies the need to create mechanisms so that individuals can control their personal information and demand the removal of harmful content.

It is warned that legislation must also keep pace with technological innovations to avoid gaps that allow abuses, as according to Lassalle (1998), the Constitution must reflect the social and economic reality of its time, ensuring effective protection against violations of fundamental rights.

Rodotà (2008) emphasizes that privacy must be safeguarded as an essential right in the surveillance society. The interaction between the State and corporations in the management of personal information must follow democratic principles, preventing citizens from being reduced to mere objects of control.

Another relevant aspect is digital abandonment, in which the excessive exposure of children and adolescents on the internet highlights the need for greater parental surveillance and regulation. Martin (2024) argues that the principle of full protection requires that both the State and companies ensure the digital safety of minors.

The data economy and business models based on the exploitation of personal information must also be critically analyzed. In this regard, Holmes and Sunstein (2019) point out that individual freedom depends directly on effective regulations, because without them, the economic power of companies can compromise individuals' self-determination.

Therefore, contemporary society faces constant challenges in balancing technological innovation and fundamental rights. As emphasized by dos Reis Silva (2021), the positivization of data protection as a fundamental right is essential to ensure that digital advances occur in a fair and ethical manner, safeguarding the dignity of citizens.

5 IMPACTS OF SURVEILLANCE ON FUNDAMENTAL RIGHTS

Mass surveillance promoted by companies and governments has raised complex questions about the protection of personality rights and privacy in the digital age. The indiscriminate collection of personal data through electronic devices and digital platforms compromises individual autonomy and creates an environment of constant monitoring. As highlighted by Alberti (2022), security is often used as a justification for the expansion of surveillance, but this practice can result in the restriction of fundamental rights.

Privacy, traditionally considered an inalienable right, has been relativized in the face of technological advances and the demands of the digital market. Discussing this matter, Canavez, Santos, and Mendes (2022) point out that the growth of the information society requires the recognition of new fundamental rights, including the right to the protection of personal data. The regulation of these rights is essential to prevent abuses and ensure that individuals maintain control over their information.

The issue of the right to be forgotten emerges as a contemporary challenge, especially in the context of the internet. Corrêa and Fagundes Filho (2022) discuss how the neutrality of the worldwide computer network impacts the protection of personal data, highlighting that the perpetuation of information can be harmful to individuals' dignity. Thus, the possibility of deleting outdated or harmful records becomes a fundamental aspect of the protection of personality.

Surveillance capitalism, a concept addressed by Silva (2021), transforms personal data into a commodity, exploiting private information for economic purposes. This model compromises individuals' sovereignty over their own information and reinforces social inequalities, since control over data is largely held by large technology corporations.

The use of disruptive technologies has deepened the challenges related to surveillance, particularly with regard to facial recognition in public spaces. Figueiredo et al. (2021) highlight that the collection and mass processing of biometric data represent an instrument of state and corporate control, potentially compromising individual freedoms and generating automated discrimination.

The constitutional essence of privacy protection is debated by Lassalle (1998), who argues that an effective constitution must reflect the social needs of its time. In this sense, the inclusion of data protection as a fundamental right reflects the evolution of society and the need to safeguard citizens against technological abuses.

Digital surveillance also impacts vulnerable groups, such as children and adolescents. Martin (2024) emphasizes that digital abandonment and the lack of an adequate duty of parental surveillance can expose minors to significant risks, requiring more effective public policies to ensure child protection in the digital environment.

Democracy is also affected by this scenario, as argued by Monteagudo (2021), who discusses the risks of ubiquitous surveillance for democratic institutions. Excessive monitoring of the population can undermine freedom of expression and inhibit political participation, weakening democratic principles.

Rodotà (2008) explores how life in the surveillance society impacts individual rights, warning of the need for a balance between security and freedom. For the author, it is essential that States implement mechanisms of regulation and control over the collection and use of personal data.

The implementation of facial recognition technologies is a growing concern. Silva (2022) discusses the implications of the use of these tools in public surveillance systems, highlighting the risk of privacy violation and the possibility of errors in the identification of individuals, which may result in injustices.

The right to be forgotten is a controversial topic in Brazilian jurisprudence. Siqueira et al. (2023) analyze the (in)applicability of this right in the legal system, demonstrating that the lack of clear regulation can generate conflicts between freedom of expression and the protection of privacy.

Holmes and Sunstein (2019) argue that the guarantee of fundamental rights depends on the existence of an efficient regulatory structure, aimed at data

protection, which requires robust legislation and oversight to prevent abuses by the private sector and the State.

Verbicaro (2021) highlights that the Brazilian Internet Civil Rights Framework (*Marco Civil da Internet*) still presents gaps in the regulation of artificial intelligence and automated decision-making mechanisms, requiring improvements to ensure transparency and accountability of the agents involved.

Resistance to this dynamic demands joint action between civil society, governments, and regulatory institutions, promoting greater transparency and responsibility in the use of personal information.

6 CHALLENGES AND PERSPECTIVES FOR THE FUTURE

The growing digitalization of society has driven the need for more effective regulations to address the challenges posed by mass surveillance. The absence of robust normative frameworks compromises the protection of fundamental rights, such as privacy and informational self-determination. According to Alberti (2022), public security is often used as a justification for the expansion of state and corporate surveillance, without a proper balance between protection and individual freedom. Thus, it becomes essential to create policies that limit the collection and indiscriminate use of personal data.

The evolution of digital rights reflects the urgency of recognizing new fundamental guarantees in the information society. Canavez, Santos, and Mendes (2022) argue that privacy and data protection have come to be considered essential rights for the exercise of digital citizenship. However, the realization of these rights still encounters structural and legislative barriers, requiring a collective effort among the State, companies, and civil society to ensure that norms keep pace with technological advancement without compromising individual freedoms.

In the context of the surveillance society, net neutrality and the protection of personal data are highly relevant themes. Corrêa and Fagundes Filho (n.d.) highlight that the implementation of regulations ensuring a more democratic and secure digital environment is fundamental to mitigating the impacts of hyperconnectivity. The lack of transparency in the collection and use of personal information by internet service providers compromises the right to privacy, demanding greater oversight and regulation.

The positivization of data protection as a fundamental right emerges as an essential mechanism to ensure greater legal certainty for citizens. According to Silva (2021), the consolidation of this right at the constitutional level is a response to the growing economic exploitation of personal data, especially in the context of surveillance capitalism. Without a solid legal basis, individuals remain vulnerable to the commodification of their information and the misuse of their data.

The regulation of state surveillance must take into account the need for balance between security and freedom. Figueiredo et al. (2021) emphasize that the technological empowerment of the surveillance State has direct implications for the constitutional right to privacy. Thus, the implementation of control and oversight

mechanisms becomes indispensable to prevent abuses and ensure that data collection meets strict criteria of necessity and proportionality.

The debate on ethics and transparency in digital surveillance is crucial to ensure more responsible governance of emerging technologies. Lassalle (1998) highlights that the Constitution reflects social reality and must evolve according to technological and cultural transformations. Thus, the updating of normative frameworks is necessary to ensure that democratic principles are preserved in a scenario of growing digital monitoring.

The regulation of disruptive technologies, such as facial recognition, also demands a more careful approach. Silva (2022) warns that the indiscriminate use of this type of technology in public spaces can compromise the effectiveness of the right to privacy, reinforcing discriminatory practices and expanding state surveillance without proper social control. Thus, policies that establish clear limits for the use of these tools are fundamental to ensuring their application in an ethical and responsible manner.

Holmes and Sunstein (2019) emphasize that individual freedom is intrinsically linked to the existence of regulations that guarantee rights and duties in the digital environment. Thus, the development of stricter norms on the collection, storage, and sharing of data is essential to ensure the dignity and autonomy of citizens.

Therefore, the creation of a solid and up-to-date regulatory framework must be accompanied by a broad public debate on the impacts of digital surveillance. Souza and Lima (2021) argue that the participation of civil society in the formulation of data protection policies is a determining factor for building a more transparent and democratic model. Only through dialogue and cooperation between different sectors will it be possible to face the challenges of digital surveillance and ensure the realization of fundamental rights in the information age.

7 FINAL CONSIDERATIONS

The present analysis has allowed an understanding of the complex challenges imposed by the surveillance society in the digital age, highlighting the profound impacts of the collection and mass processing of data on fundamental rights. Throughout the study, the limits of privacy, the advancement of monitoring technologies, and the urgency of creating effective regulations that protect citizens in a scenario marked by hyperconnectivity and the intensive use of personal data were explored.

The growing interconnectivity, driven by sophisticated algorithms and artificial intelligence systems, has intensified surveillance practices by governments and corporations. This makes an ethical, legal, and political debate on the direction of digital governance indispensable, demanding greater transparency in the formulation and application of data control policies. Surveillance mechanisms, although often justified on grounds of public security, cannot be turned into instruments of repression, manipulation, or social exclusion.

One of the great contemporary dilemmas lies in the effort to find a legitimate balance between security and privacy. The justification of monitoring as a tool for preventing crimes and threats to public order cannot be used as a subterfuge for the suppression of individual guarantees. At the same time, the absence of effective oversight and accountability mechanisms on the part of public authorities and private companies exposes individuals to risks of exposure, discrimination, and disinformation. It is therefore essential to establish clear norms that ensure the principles of purpose, proportionality, and data minimization, safeguarding the dignity and autonomy of users in the digital environment.

Data protection must be regarded as a fundamental right in the full sense, with constitutional status and effective operationalization. To this end, it is imperative to strengthen public policies that ensure its implementation, as well as the training of oversight bodies, such as data protection authorities and digital public defender's offices. The legal system must evolve to offer not only sanctions for abuses, but also guarantees of redress and preventive mechanisms.

Beyond the normative perspective, the importance of digital citizenship as a central element in resisting excessive surveillance stands out. The informational empowerment of citizens, through critical education and awareness of their rights in the digital space, is an indispensable condition for building a culture of privacy. In this sense, teaching about data protection and privacy in schools, universities, and public spaces should be incorporated as cross-curricular content, fostering an active stance of protection and demand for rights on the part of society.

Another aspect worth highlighting is the international comparison of regulatory frameworks. Experiences such as the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and South Africa's Protection of Personal Information Act (POPIA) demonstrate different regulatory paths, with varying degrees of success and effectiveness. From these experiences, it is possible to identify best practices and fundamental principles, such as privacy by design, accountability, and the right to data portability. The comparative analysis also reveals the need to adapt national norms to the cultural, economic, and technological specificities of each country, ensuring that fundamental rights are not subordinated to economic or political interests.

Digital surveillance, beyond being a legal problem, is also an ethical and civilizational issue. The advancement of technologies such as facial recognition, real-time tracking, automated listening, and social media monitoring challenges the limits of what is understood as freedom, intimacy, and anonymity. In democratic societies, the protection of spaces of personal autonomy is indispensable for the construction of identities, political dissent, and cultural plurality. Excessive surveillance, in turn, tends to homogenize behaviors and establish a logic of control and punishment incompatible with republican values.

From an institutional perspective, it is necessary to ensure that data protection authorities have functional independence, adequate technical and budgetary resources, and effective channels of interaction with citizens. The enforcement of

digital rights requires a robust institutional apparatus, capable of overseeing, applying sanctions, conducting investigations, and promoting a culture of data protection. In this regard, the role of the Public Prosecutor's Office, the Judiciary, and civil society organizations is central to ensuring compliance with legislation and curbing abusive practices.

Corporate action also needs to be rethought. Corporate responsibility in the ethical use of data must go beyond formal compliance with laws. It is necessary to adopt compliance policies that include external audits, algorithmic review mechanisms, technology ethics committees, and ongoing training programs. Companies that collect, store, and use data on a massive scale must make transparent commitments to society, including regarding the explainability and criteria used in content personalization, dynamic pricing, profile classification, and automated exclusions.

In the educational context, the promotion of digital literacy is essential so that individuals understand how their data are collected, processed, and used, and so that they can exercise their rights in an informed and conscious manner. This ranges from understanding how cookies and algorithms work to knowledge about the rights of access, rectification, objection, and data erasure. The development of digital skills is not only a tool for inclusion, but a strategy of resistance to social control and of strengthening citizenship.

With regard to the future, it is foreseeable that surveillance practices will become increasingly sophisticated, integrated, and ubiquitous. Emerging technologies such as 6G, quantum computing, the internet of things, and neurotechnology expand the capacity for data capture and inference, including data related to brain patterns, unconscious behaviors, and emotions. This demands a continuous review of regulatory frameworks and a profound reflection on the limits of what is acceptable in terms of technological intervention in private life.

Facial recognition technologies, for example, have been used for various purposes, such as predictive policing, border control, candidate selection for employment, and credit granting. Without clear criteria of proportionality, transparency, and auditing, these systems can reinforce discriminatory biases, criminalize vulnerable populations, and perpetuate structural inequalities. It is urgent to establish strict ethical and legal limits on the implementation of these tools, ensuring that their use is always subordinated to the legitimate public interest and fundamental rights.

Additionally, the use of artificial intelligence in public decision-making - such as granting benefits, patient triage, or resource allocation - must be guided by principles of algorithmic justice, impartiality, auditability, and explainability. The risk of automated discrimination is real and must be addressed with rigorous public policies, including mandatory algorithmic impact reports, prior public consultation, and contestation mechanisms.

Digital surveillance also raises important questions about the limits of national sovereignty. Often, the data of a country's citizens are processed on servers

located abroad, under the jurisdiction of other legal systems. This requires international agreements that ensure respect for transnational fundamental rights and interoperability between data protection systems. International cooperation is crucial to address cross-border privacy violation practices, such as cyber espionage, illegal data trade, and targeted political advertising.

Finally, it is essential that the debate on digital surveillance is not restricted to experts and institutions. Citizen participation in the formulation of laws, policies, and technical standards is essential to ensure that technologies respect diversity, democratic values, and human rights. Algorithmic transparency and digital justice will only be effective if accompanied by public spaces for deliberation, social control, and co-responsibility.

Therefore, the surveillance society imposes challenges that demand rapid, assertive, and sustainable responses. The search for balance between technological innovation, security, and the protection of fundamental rights must be a continuous commitment, anchored in ethics, legality, and social justice. The strengthening of digital governance, combined with the active participation of civil society, institutional capacity-building, and the creation of an efficient normative ecosystem, will be decisive in ensuring that the digital age develops in a fair, plural, and democratic manner, preserving the freedom, diversity, and dignity of individuals.

4 REFERENCES

- ALBERTI, Marcia de Oliveira Souza. *Mass surveillance and security. Public Security, Citizenship and Human Rights: research, reports and reflections*, v. 2, p. 116, 2022.. DOI: <https://doi.org/10.47573/aya.5379.2.109.9>
- CANAVEZ, Luciana Lopes; SANTOS, Isadora Beatriz Magalhães; MENDES, Daniella Salvador Trigueiro. *Surveillance, data protection and privacy: the recognition of new fundamental rights in the information society*.. Revista de Direito, Governança e Novas Tecnologias, v. 8, p. 68-86, 2022.
- CORRÊA, Paulo Sérgio Gaspar; FAGUNDES FILHO, Antonio. *Neutralidade da rede mundial de computadores e os impactos da proteção de dados pessoais na sociedade de vigilância.(Academic work in publication phase)*.
- FIGUEIREDO, Letícia Fraga de et al. *The technological empowerment of the surveillance State vis-à-vis the constitutional right to privacy and data protection: the collection and processing of personal data as an instrument of control. Brazilian Journal of Public and International Policies*, v. 6, n. 1, 2021.
- LASSALE, Ferdinand. *The Essence of the Constitution*. Trad.: Walter Stonner. 4. Ed. Rio de Janeiro: Lumen Juris, 1998.
- MARTIN, Júlia Saes. *Digital abandonment and the duty of parental surveillance under the principle of integral protection of children*. 2024.
- MONTEAGUDO, Ricardo. *Democracy in times of ubiquitous surveillance*. Quaestio Iuris (QI), v. 14, n. 4, 2021.. DOI: <https://doi.org/10.12957/rqi.2021.62818>
- RODOTÁ, Stefano. *Life in the Surveillance Society: privacy today* . Trad.: Danilo Doneda a Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.
- SILVA, Guilherme Brito Araújo da. *Applicability of disruptive facial recognition technologies in public surveillance systems in Brazil: implications for the effectiveness of the constitutional right to privacy*. 2022. Course conclusion work.

SILVA, Lucas dos Reis. *Data protection and its need for positivization as a fundamental right in the era of surveillance capitalism*. Repository of Course Conclusion Works - Faculty of Law, Federal University of Minas Gerais, 2021.

SIQUEIRA, Dirceu Pereira et al. *Personality rights and the "Ainda Curi" judgment: analysis on the (in)applicability of the right to be forgotten in the Brazilian legal system*. *Journal of Constitutionalization of Brazilian Law*, v. 6, n. 1, p. 1-25, 2023.

SOUZA, Diego Chagas de; LIMA, João Vitor Sangiacomo Meira. *The scope of consent in the protection of personal data: perspectives on the surveillance society in the information age*. *Electronic Journal of PGE-RJ*, v. 4, n. 3, 2021. DOI: <https://doi.org/10.46818/pge.v4i3.242>

STEPHEN, Holmes. SUSTEIN, Cass R. *The Cost of Rights: why freedom depends on taxes*. Trad.: Marcelo Brandão Cipolla. São Paulo: Martins Fontes, 2019.

VERBICARO, Dennis. *Challenges in the regulation of algorithms under the Brazilian Internet Civil Rights Framework*. *Journal of Law, Innovation and New Technologies*, [S.l.], 2022.

ZUBOFF, Shoshana. *The Age of Surveillance Capitalism: the fight for a human future at the new frontier of power*. Trad.: George Schlesinger. São Paulo: Intrínseca, 2021.