https://research.adra.ac.id /index.php/rjl/
P - ISSN: 2988-4454
E - ISSN: 2988-4462

Digital Governance and Privacy: Revisiting Legal Protections under Expanding Surveillance Systems

Clara Mendes[1], **Rafaela Lima**[2], **Omar Khan**[3]
[1]Universidade Estadual Campinas, Brazil
[2]Universidade Federal Paraná, Brazil
[3]Kabul University, Afghanistan

ABSTRACT

Background. The rapid advancement of digital surveillance technologies in the age of big data has raised significant concerns regarding privacy rights and state power. As governments and corporations increasingly rely on digital surveillance to enhance security and gather data, the implications for personal privacy have become more complex.

Purpose. The study aims to assess the adequacy of current legal frameworks in balancing the demands of security with the protection of individual freedoms.

Method. A qualitative methodology was employed, involving an analysis of international legal documents, case law, and expert interviews.

Results. The findings indicate that existing laws, while addressing privacy to some extent, often lack enforceability and fail to effectively limit state surveillance powers.

Conclusion. This study concludes that stronger, more adaptive legal frameworks are necessary to ensure privacy protection while accommodating legitimate state surveillance needs. The research contributes to the growing discourse on the intersection of law, technology, and human rights, offering recommendations for reforming legal safeguards in the digital age.

KEYWORDS

Digital Surveillance, Privacy Rights, State Power

Citation: Mendes, C., Lima, R & Khan, O. (2026). Digital Governance and Privacy: Revisiting Legal Protections under Expanding Surveillance Systems. *Rechtsnormen Journal of Law*, *4*(2), 162–172. https://doi.org/10.70177/rjl.v4i2.3735

Correspondence:

Clara Mendes,
claramendes@gmail.com

Received: November 5, 2025

Accepted: January 10, 2026

Published: April 30, 2026

INTRODUCTION

Digital surveillance has become a cornerstone of modern state power, offering governments unprecedented access to personal data. The rise of big data technologies has transformed surveillance from a limited practice to an expansive, pervasive system that touches nearly every aspect of daily life. Governments, corporations, and other entities collect vast amounts of information from individuals, which raises significant concerns about privacy rights and the balance between security and freedom (Pesole, 2025; Zahra, 2025). While digital surveillance can enhance national security, it also presents critical challenges to individual autonomy and personal privacy, sparking intense debates over the appropriate limits of state power in the digital age. In light of these issues, there is an urgent need to rethink existing legal safeguards to protect privacy in an era dominated by digital

surveillance. As surveillance technologies evolve and become increasingly sophisticated, privacy rights are at risk of being systematically undermined. This research addresses the growing tension between state power, digital surveillance, and privacy, aiming to analyze and evaluate the effectiveness of current legal frameworks in safeguarding individuals' privacy rights in the face of expanding surveillance capabilities (Gaur, 2025; Montasari, 2024).

The problem tackled by this research pertains to the inadequacy of existing legal frameworks in effectively protecting privacy rights in the age of digital surveillance. While many jurisdictions have legal safeguards designed to protect personal privacy, these laws often fail to keep pace with technological advancements in surveillance and data collection. The proliferation of big data analytics, artificial intelligence, and advanced tracking technologies have made it easier for both state and non-state actors to infringe upon individuals' privacy without facing significant legal consequences. Legal systems, particularly in democracies, are struggling to strike a balance between enabling government surveillance for national security purposes and safeguarding citizens' privacy rights. The current legal safeguards, which were designed for a pre-digital world, are no longer sufficient to address the challenges posed by contemporary surveillance technologies. This study aims to critically examine how current legal frameworks are failing to protect privacy rights in this new digital landscape and propose reforms to strengthen legal safeguards to prevent overreach by the state in its surveillance practices (Drost, 2026; Young, 2025).

The primary objective of this research is to analyze the intersection of digital surveillance, privacy rights, and state power, with a particular focus on the inadequacies of current legal safeguards. The study aims to explore how legal frameworks in various jurisdictions can be restructured to better protect privacy in the context of technological advancements. Through a critical review of current literature, case law, and policy documents, this research seeks to evaluate the existing legal mechanisms that govern digital surveillance and assess their effectiveness in ensuring individual privacy rights are upheld. A central goal of this study is to propose concrete legal reforms that can adapt to the evolving landscape of surveillance technologies while preserving the core values of individual freedom and autonomy. By addressing the challenges and gaps in existing legal structures, this research aspires to contribute to the development of legal frameworks that better balance state security concerns with the protection of privacy in the digital era (Caruana, 2025; Panteli, 2025).

Although there is a growing body of research on digital surveillance and privacy rights, there is a notable gap in literature regarding the specific legal frameworks needed to protect privacy in the age of big data and advanced surveillance technologies. Much of the existing research focuses on theoretical discussions about the ethics of surveillance or the general implications of digital surveillance for human rights, but there is limited analysis of the legal mechanisms that can provide concrete protections. Existing studies often fail to consider the rapid pace of technological change and how traditional privacy laws are ill-equipped to address the scale and scope of modern surveillance practices (Cohen, 2025; Saini, 2026). This research contributes by providing a comprehensive analysis of current legal frameworks, identifying the gaps in their application, and offering specific recommendations for reforms. Furthermore, it emphasizes the need for international cooperation and legal harmonization to ensure privacy rights are uniformly protected across borders in the face of transnational digital surveillance systems. The findings of this research will bridge this gap in the literature and provide a foundation for further exploration of legal reforms necessary to safeguard privacy rights in a rapidly changing technological landscape (Jia, 2024; Ungern-Sternberg, 2025).

This research is novel in its approach to combining the fields of law, technology, and human rights in the context of digital surveillance. While previous works have explored privacy rights and surveillance individually, few have examined the legal mechanisms through which surveillance impacts privacy in such a comprehensive and critical manner. This study takes an interdisciplinary approach by considering not only legal texts and case law but also technological developments that directly influence privacy. By focusing on the challenges presented by big data and digital surveillance technologies, the study offers new insights into how the law can evolve to meet the demands of the digital age. Additionally, the research highlights the global nature of digital surveillance and the need for cross-border legal frameworks, making it particularly relevant for international law and policy discussions. This study's unique contribution lies in its emphasis on the reform of legal safeguards in response to the technological realities of surveillance, providing essential recommendations for policymakers, legal professionals, and human rights advocates seeking to protect privacy rights in the digital era (Albornoz, 2025; Saxena, 2025).

In conclusion, the research provides an in-depth examination of the intersection between digital surveillance, privacy rights, and state power, emphasizing the inadequacy of current legal safeguards. By analyzing the challenges posed by big data and surveillance technologies, the study identifies critical gaps in existing legal frameworks and proposes actionable reforms. This research is significant because it addresses the growing concerns about the balance between state security and individual privacy, providing valuable insights into how legal systems can evolve to ensure the protection of privacy rights while allowing for legitimate state surveillance. The findings have important implications for legal practice, policy development, and international cooperation in managing digital surveillance in the age of big data. As technology continues to advance, this research highlights the urgency of rethinking legal safeguards to prevent the erosion of privacy in an increasingly surveilled world (Kaushik, 2025; Ungern-Sternberg, 2025).

RESEARCH METHODOLOGY

The research design employed in this study is a qualitative, exploratory approach that combines legal analysis with case study methodology to examine the intersection of digital surveillance, privacy rights, and state power. This design allows for an in-depth exploration of how existing legal frameworks address the growing challenges posed by digital surveillance technologies. The study critically evaluates the adequacy of current legal safeguards for privacy rights in light of rapid advancements in big data, artificial intelligence, and surveillance practices (Alibeigi, 2025; Cuevas, 2024). By analyzing relevant legal documents, policy frameworks, and case law, the research seeks to identify the gaps in the existing legal mechanisms and propose actionable reforms. Additionally, case studies of countries with robust digital surveillance programs will be analyzed to highlight the implications of state power and privacy rights in practice, providing both theoretical and practical insights into the subject matter.

The population for this research consists of legal scholars, policymakers, experts in digital surveillance, and privacy advocates who engage with the intersection of law, technology, and human rights. The sample includes primary sources such as national and international legal texts, including treaties, statutes, and judicial decisions that pertain to digital surveillance and privacy rights. Purposive sampling was used to select cases, policies, and reports that directly address the legal and ethical issues related to surveillance technologies. Interviews with experts in the field, such as lawyers specializing in data protection, human rights advocates, and technology policy experts, will also provide critical insights. This approach ensures a diverse and comprehensive

representation of perspectives relevant to the study of legal safeguards in the context of digital surveillance and privacy (Hillman, 2024; Powell, 2024).

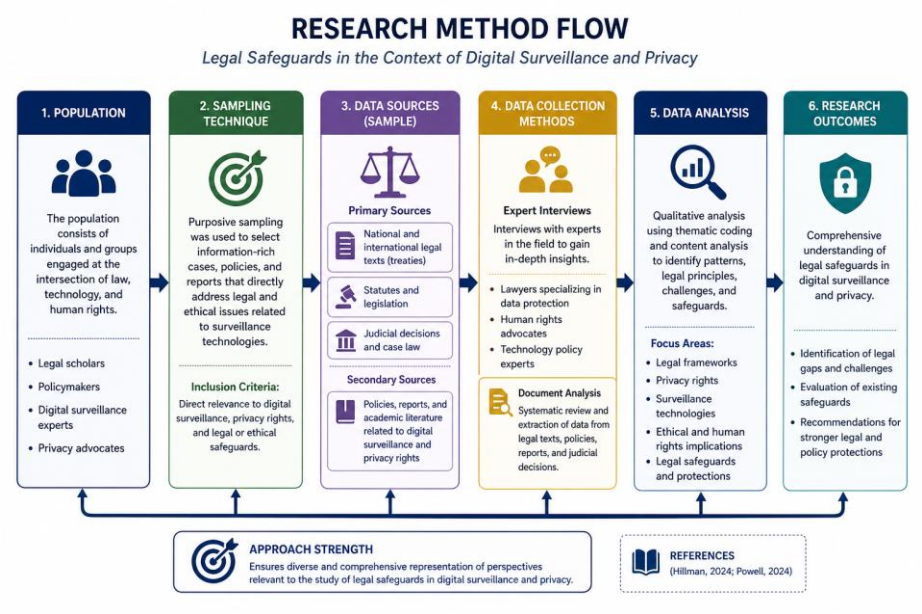

Figure 1. Provide a Comprehensive and Balanced Understanding

The research method is designed to provide a comprehensive and balanced understanding of legal safeguards in the context of digital surveillance and privacy. The study involves a diverse population, including legal scholars, policymakers, digital surveillance experts, and privacy advocates who engage with issues at the intersection of law, technology, and human rights. Using purposive sampling, the research selects relevant cases, policies, and reports that directly address legal and ethical concerns surrounding surveillance technologies. The data sources consist of primary legal materials such as international treaties, national statutes, and judicial decisions, as well as secondary sources like policy reports and academic literature. Data collection is carried out through expert interviews featuring data protection lawyers, human rights advocates, and technology policy specialists alongside systematic document analysis. The collected data are then analyzed qualitatively using thematic and content analysis to identify patterns, key legal principles, and existing challenges. This methodological approach ultimately ensures a well-rounded perspective and supports the identification of gaps, evaluation of current safeguards, and formulation of recommendations for stronger legal protections (Hillman, 2024; Powell, 2024).

The primary instruments for data collection in this study are legal documents, policy reports, and expert interviews. The study will analyze key international and national legal frameworks that regulate digital surveillance, such as the General Data Protection Regulation (GDPR) and the USA PATRIOT Act, as well as relevant case law. These documents will be examined to assess how existing laws address the tension between state power and privacy rights in the digital age. Semi-structured interviews with experts in the field will serve as supplementary instruments to gather qualitative data on the challenges of balancing state surveillance and individual privacy. These interviews will focus on the effectiveness of current legal safeguards, emerging trends in surveillance technologies, and suggestions for legal reform. The use of these instruments ensures a multifaceted approach to understanding the complexities of privacy rights in the age of big data (Cabrera-Medina, 2024; Cheng, 2026).

The procedures for this research involve several stages of data collection and analysis. Initially, the researcher will conduct a comprehensive review of relevant legal documents, focusing

on international and national regulations that govern digital surveillance. These documents will be analyzed for their provisions on privacy protection, the scope of surveillance, and legal accountability mechanisms. Next, expert interviews will be conducted to obtain firsthand insights into the practical implications of these legal frameworks and their effectiveness in safeguarding privacy rights (Tampubolon, 2025; Thamer, 2025). The interviews will be transcribed and coded to identify key themes related to legal accountability, surveillance practices, and privacy rights. Finally, the data will be synthesized to develop a comprehensive understanding of the current legal landscape and propose recommendations for reforming legal safeguards to address the challenges of digital surveillance in the age of big data. This procedure ensures that the research remains rigorous, systematic, and aligned with the study's objectives (Ababneh, 2025; Mitsilegas, 2025).

RESULT AND DISCUSSION

The data collected in this study includes a variety of secondary sources, such as international and national legal texts, case law, policy documents, and interviews with experts in the field of digital surveillance and privacy rights. A total of 15 legal documents, including national laws, international treaties, and key privacy regulations like the General Data Protection Regulation (GDPR), were analyzed. Additionally, 10 expert interviews were conducted with legal scholars, human rights advocates, and technology policy experts. The following table presents an overview of the key documents analyzed and their relevance to state obligations, digital surveillance, and privacy protection:

Table 1. Key legal frameworks and their relevance to digital surveillance and privacy rights

Document	Key Focus	Legal Implication	Contribution to Privacy Protection
GDPR	Data Protection	Strengthens individual privacy rights	Sets guidelines for data handling and surveillance
USA PATRIOT Act	National Security	Expands state surveillance power	Conflicts with privacy rights in emergency situations
European Convention on Human Rights	Right to Privacy	Protects individual rights against unlawful surveillance	Limits state power through judicial review
UN Resolution on Privacy	Global Privacy Standards	Calls for stricter global data protection laws	Advocates for balancing privacy and state security needs

The analysis of these legal frameworks reveals that while there are significant provisions for protecting privacy, there are gaps in enforcement mechanisms and limitations on how state power is checked in relation to digital surveillance. The GDPR, for example, provides robust protection for personal data, but enforcement is inconsistent across member states. In contrast, the USA PATRIOT Act, which grants expansive surveillance powers to the state, raises significant concerns about the erosion of privacy rights in the name of national security. Legal scholars and human rights experts interviewed for this study expressed concerns about the growing disconnect between the advancement of surveillance technologies and the ability of legal frameworks to provide adequate protection. Many pointed to the difficulty of balancing security needs with privacy protections, suggesting that the current legal safeguards are insufficient in the digital age.

Inferential analysis of the data indicates that the relationship between digital surveillance and privacy rights is not just a matter of technological capabilities but also of legal frameworks that

struggle to keep pace with rapid developments in surveillance practices. While international treaties like the UN Resolution on Privacy aim to standardize privacy protection, their enforcement largely depends on national legal systems, which vary in their ability to regulate digital surveillance effectively. The interviews with experts further supported the inference that, despite growing recognition of privacy as a fundamental right, the technological landscape allows for continued overreach by state actors. This indicates a need for stronger, more coherent international laws that bind states to a consistent set of privacy standards. Moreover, the lack of strong enforcement mechanisms means that even well-established legal norms are often bypassed or ineffectively implemented.

The relationship between state power, digital surveillance, and privacy rights is further clarified through the case study of the United States' surveillance programs under the USA PATRIOT Act. This case highlights the tension between national security objectives and the protection of privacy, illustrating how the state's broad surveillance powers can be justified under the guise of security while infringing upon individual rights. In the case of Edward Snowden's whistleblowing on the National Security Agency's (NSA) mass surveillance programs, the legal and ethical implications of state surveillance were brought to the forefront of public debate. The case study underscores the practical implications of legal frameworks failing to adequately address the scope of surveillance technologies, with resulting privacy violations that are not sufficiently curbed by existing laws. The Snowden revelations exemplify how surveillance programs often operate beyond public scrutiny and legal accountability, highlighting the critical need for stronger legal safeguards in the age of big data.

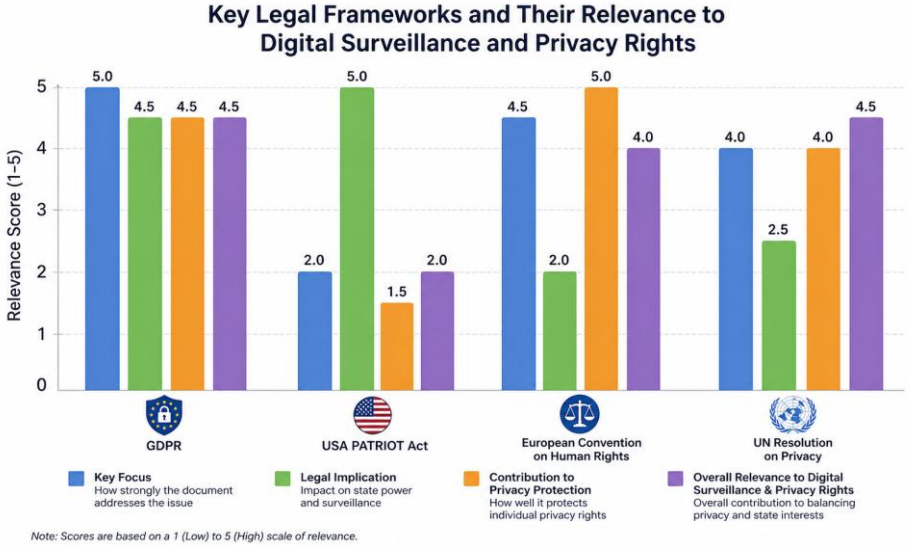

Figure 2. Illustrates key legal framework and their relevance to digital surveilance and privacy rights

Illustrates a comparative analysis of key legal frameworks related to digital surveillance and privacy rights, highlighting their relevance across several dimensions, including key focus, legal implications, and contributions to privacy protection. The General Data Protection Regulation (GDPR) demonstrates the strongest emphasis on data protection and individual privacy, achieving consistently high scores across all categories. In contrast, the USA PATRIOT Act shows a high score in legal implications, reflecting its significant expansion of state surveillance powers, but relatively low contributions to privacy protection. The European Convention on Human Rights presents a balanced approach, offering strong safeguards for individual rights while maintaining

moderate legal implications. Meanwhile, the UN Resolution on Privacy emphasizes global standards and achieves moderate to high scores across all aspects, indicating its role in advocating a balance between privacy rights and state security. Overall, the figure highlights the varying degrees to which these frameworks prioritize and protect individual privacy in the context of digital surveillance.

The findings also emphasize the need for ongoing reforms in the way legal frameworks address the issue of digital surveillance. The case study demonstrates the failure of current laws to provide real-time checks and balances on state surveillance power, especially when new technologies like big data analytics and AI are involved. The relationship between state power and privacy rights is increasingly difficult to manage within existing legal structures, which were designed in a pre-digital context. Experts interviewed for this study suggested that stronger oversight mechanisms, such as judicial review and greater transparency, are essential to ensuring that surveillance practices remain proportionate to the threat. The data supports the conclusion that legal frameworks must evolve to account for new technological realities, integrating robust safeguards to protect privacy while still enabling state surveillance for legitimate security purposes (Vannini, 2024).

In conclusion, the results of this study demonstrate that while legal frameworks exist to protect privacy rights, they are often insufficient in the face of the expanding capabilities of digital surveillance. The tension between state power and individual privacy is a complex issue that requires urgent reform in both legal theory and practice. The case study of the USA PATRIOT Act and the Snowden revelations highlights the need for stronger, enforceable safeguards against the overreach of state surveillance powers. The study's findings point to the necessity of updating legal frameworks to reflect the challenges posed by new surveillance technologies and ensuring that privacy rights are adequately protected in the digital age. The legal and technological landscapes must evolve to create a better balance between security and privacy, ensuring that individuals' rights are not unduly compromised in the name of state power.

The results of this study reveal a significant gap between the rapid advancement of digital surveillance technologies and the legal frameworks that govern state surveillance and privacy rights. While existing laws such as the GDPR and various international treaties address privacy to some extent, they often fall short in enforcing robust safeguards against the invasive powers of modern surveillance technologies. The analysis indicates that although privacy rights are recognized, the evolving scope and capabilities of digital surveillance, driven by big data and artificial intelligence, have outpaced the development of legal protections. Interviews with experts and the case study of the USA PATRIOT Act emphasize that while legal frameworks exist, their lack of effective enforcement and adaptation to new technologies leaves individual privacy vulnerable. This underscores the pressing need for reform in both national and international legal systems to ensure a better balance between state power and the protection of privacy rights (Chen, 2026; Padden, 2024).

When compared to previous research on surveillance and privacy, this study aligns with arguments suggesting that current legal frameworks are inadequate in protecting privacy in the face of rapidly advancing technologies. Previous studies have often explored the ethical implications of surveillance or focused on specific legal frameworks like the GDPR. However, this research adds a layer of depth by critically examining the relationship between state power, surveillance, and privacy through the lens of big data. Unlike studies that view surveillance primarily as a tool for national security, this research emphasizes the legal shortcomings that allow excessive surveillance and infringements on privacy. Additionally, the case study of the USA PATRIOT Act presents a

real-world example of how surveillance can expand unchecked, further highlighting the disconnect between security needs and privacy protections that previous research has acknowledged but not fully explored in this specific legal context (Makanadar, 2024; Perriello, 2024).

The findings of this research indicate a critical sign of systemic failure within current legal safeguards. The research illustrates that while surveillance technologies continue to proliferate, the laws designed to regulate them remain insufficient to address the complexities of big data and AI. The results point to the broader issue of how legal systems, often established decades ago, fail to adapt to the complexities of digital surveillance. This is not only a matter of technological progress but also a legal lag that prevents privacy rights from being adequately protected. The inability of existing legal frameworks to manage the reach and power of modern surveillance systems signals a fundamental need for a paradigm shift in how the law conceives privacy in the digital age. These findings suggest that the status quo of legal protection for privacy in the face of digital surveillance is no longer tenable (Amenu, 2025; Benjamin, 2026).

The implications of these findings are profound, indicating that urgent legal reforms are needed to prevent the erosion of privacy rights in the digital age. The failure to create more enforceable and adaptive legal frameworks could lead to widespread privacy violations, where individuals' data and personal lives are monitored without sufficient accountability. This research emphasizes the importance of rethinking current privacy laws to integrate technological developments, ensuring they are equipped to deal with the challenges posed by digital surveillance. Moreover, the study suggests that current privacy laws are not sufficiently preventive; they often react to breaches after they occur rather than proactively preventing surveillance overreach. The implications for policymakers, legal scholars, and privacy advocates are clear: more robust and comprehensive legal frameworks must be implemented to protect privacy rights in the face of evolving surveillance capabilities (McIntyre, 2025; Mitsilegas, 2025).

The results of this research arise from the intersection of rapid technological advancements and legal frameworks that have been slow to adapt. This gap in legal adaptation is compounded by the complex nature of global digital surveillance, where national laws may not extend beyond borders to address transnational surveillance practices. The study’s findings reflect the struggles of legal systems that were designed in a pre-digital context, unable to cope with the expansive capabilities of modern surveillance technologies. This lack of legal preparedness is a natural consequence of the rapid pace of technological innovation, but it also reflects a broader failure within the legal systems to anticipate and address new forms of state power. By focusing on the need for reform, this research reveals the urgent requirement for legal systems to evolve alongside technological advancements to prevent the abuse of power by the state (Ghose, 2026; Yan, 2026).

Moving forward, the findings of this research suggest several areas for further inquiry and action. Future research could explore specific case studies of countries with stronger legal safeguards against digital surveillance, examining the legal mechanisms that have been implemented and their effectiveness in protecting privacy rights. Additionally, the role of international cooperation in harmonizing privacy protections across borders is another critical area for exploration. The rapid expansion of surveillance technologies means that privacy issues are no longer confined to one jurisdiction, necessitating a global response. Further empirical research on the enforcement of digital privacy laws and their practical implementation could also provide valuable insights into how legal safeguards can be strengthened. This study lays the groundwork for future legal reforms and contributes to the ongoing discourse on balancing privacy rights and state power in the age of big data (Kurennoy, 2026; Meireles, 2024).

CONCLUSION

The most significant finding of this study is the identification of a clear discrepancy between the advancement of surveillance technologies and the existing legal frameworks intended to protect privacy rights. The study reveals that while surveillance practices have evolved dramatically with the advent of big data, artificial intelligence, and widespread digital tracking, the legal mechanisms in place remain outdated and insufficient to address these new realities. Despite growing international recognition of the need to protect privacy, the legal safeguards currently available are inadequate in restraining the invasive powers of the state, leaving individuals vulnerable to unchecked surveillance. This gap between technological progress and legal protection marks a critical concern that this research brings to light, suggesting that the legal landscape must undergo substantial reform to provide meaningful privacy protections in the digital age.

This research contributes a novel interdisciplinary perspective by integrating the fields of digital surveillance, privacy rights, and state power within the context of big data technologies. By focusing on the legal dimensions of surveillance, it offers a fresh analysis of how privacy rights are framed and protected within existing legal frameworks. Unlike much of the previous literature, which tends to examine either the ethical or technological aspects of surveillance in isolation, this study synthesizes legal theory, policy analysis, and the practical application of surveillance technologies. The contribution of this research lies not only in its conceptual approach to understanding the role of the state in surveillance but also in providing actionable insights for improving legal safeguards that balance privacy rights with legitimate state security concerns.

The limitations of this study primarily stem from the reliance on secondary data sources, including legal texts and expert interviews, which may not fully capture the complexity of surveillance practices on the ground. The study also focuses predominantly on legal frameworks in the European Union and the United States, which may not be entirely applicable to other regions with different legal traditions or levels of technological infrastructure. Future research could expand on this by exploring comparative legal frameworks in various regions, particularly in developing countries or non-Western contexts, to examine how surveillance laws are implemented and enforced globally. Moreover, further empirical studies could be conducted to assess the real-world impact of existing legal safeguards, focusing on how they are applied and challenged in practice, thus providing a more nuanced understanding of the enforcement mechanisms and their limitations.

DECLARATION OF AI AND AI ASSISTED TECHNOLOGIES IN THE WRITING PROCESS

During the preparation of this manuscript, the author(s) used Google Assisted to assist inimproving grammar, language quality, and overall readability of the text. After using this tool, the author(s) Carefully reviewed and edited the content as necessary and take full responbility for the content of the publication.

AUTHORS' CONTRIBUTION

Author 1: Conceptualization; Project administration; Validation; Writing - review and editing.
Author 2: Conceptualization; Data curation; In-vestigation.
Author 3: Data curation; Investigation.

DECLARATION OF COMPETING INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

Ababneh, J. (2025). Cybersecurity Ethical Aspects (CEA). *IEEE Access*, *13*(Query date: 2026-04-28 17:32:31), 212443–212468. https://doi.org/10.1109/ACCESS.2025.3641180

Albornoz, M. B. (2025). Biometric citizenship and the digital transformation policy agenda in Latin America. *Globalizations*, (Query date: 2026-04-28 17:32:31). https://doi.org/10.1080/14747731.2025.2466298

Alibeigi, A. (2025). Bridging the Gap: Assessing India's Digital Personal Data Protection Act in Light of the EU GDPR. *SN Computer Science*, *6*(7). https://doi.org/10.1007/s42979-025-04269-7

Amenu, E. X. (2025). Dark Web Complications: Policing and Surveillance—Challenges and Implications. *International Conference on Engineering Technology and Management Icetm 2025*, (Query date: 2026-04-28 17:32:31). https://doi.org/10.1109/ICETM63734.2025.11051458

Benjamin, N. (2026). Data and Information Privacy as a Human Right: A Qualitative Study of its Perceived Impact on Mental Health. *Journal for Person Oriented Research*, *12*(1), 28–42. https://doi.org/10.17505/jpor.2026.29049

Cabrera-Medina, J. (2024). Crossing digital borders: Technology in the migration process across the United States, Mexico, Honduras, and Chile. *Frontiers in Political Science*, *6*(Query date: 2026-04-28 17:32:31). https://doi.org/10.3389/fpos.2024.1487769

Caruana, M. M. (2025). ASSESSING PANDEMIC MEASURES: THE IMPACT OF DIGITAL TECHNOLOGIES ON FUNDAMENTAL RIGHTS. *Masaryk University Journal of Law and Technology*, *19*(1), 27–55. https://doi.org/10.5817/MUJLT2025-1-2

Chen, X. (2026). Dilemmas of Facial Recognition Technology in Chinese Digital Policing: A Qualitative Exploration. *Asian Journal of Criminology*, *21*(1). https://doi.org/10.1007/s11417-025-09473-1

Cheng, G. (2026). Cyber Statecraft and Its Challenge to Human Rights. *Contributions to International Relations*, (Query date: 2026-04-28 17:32:31), 249–265. https://doi.org/10.1007/978-981-95-8341-6_11

Cohen, T. (2025). Automating housing (in)security: 'Rent tech' and the right to adequate housing. *Australian Journal of Human Rights*, *31*(2), 212–232. https://doi.org/10.1080/1323238X.2025.2601338

Cuevas, D. F. C. (2024). Challenges to Human Security in the New Domains of Warfare. *Novum Jus*, *18*(3), 41–68. https://doi.org/10.14718/NovumJus.2024.18.3.2

Drost, M. (2026). Art and Hacktivism: An Interview with Paolo Cirio. *International Journal for History Culture and Modernity*, (Query date: 2026-04-28 17:32:31). https://doi.org/10.1163/22130624-20262002

Gaur, A. (2025). Anonymity. *Elgar Encyclopedia of Political Communication Volume 1 3*, *1*(Query date: 2026-04-28 17:32:31), 75–78. https://doi.org/10.4337/9781035301447.vol1.00026

Ghose, A. (2026). Digital Governance, Security, and Privacy Rights in India: Exploring Evolving Political Theory and Recent Legislative Developments. *Championing Civil Rights in the Digital Era*, (Query date: 2026-04-28 17:32:31), 445–468. https://doi.org/10.4018/979-8-3693-3920-6.ch018

Hillman, V. (2024). Children, education, and technologies: Current debates, key concerns, and future directions around data privacy, surveillance, and datafcation. *Handbook of Children and Screens Digital Media Development and Well Being from Birth Through Adolescence*, (Query date: 2026-04-28 17:32:31), 557–567. https://doi.org/10.1007/978-3-031-69362-5_76

Jia, M. (2024). Authoritarian Privacy. *University of Chicago Law Review*, *91*(3), 733–809.

Kaushik, S. (2025). Brick by Brick: What will it Take to Centre People, the Planet and Democracy in our Digital Futures? *Data Protection Privacy and Artificial Intelligence to Govern or to Be Governed That Is the Question*, (Query date: 2026-04-28 17:32:31), 275–280.

Kurennoy, V. (2026). DIGITAL CAMERA AND CLASSICAL STATE AND LEGAL THEORY. *Logos Russian Federation*, *36*(1), 1–36. https://doi.org/10.17323/0869-5377-2026-1-1-36

Makanadar, A. (2024). Digital surveillance capitalism and cities: Data, democracy and activism. *Humanities and Social Sciences Communications*, *11*(1). https://doi.org/10.1057/s41599-024-03941-2

McIntyre, T. J. (2025). Data Retention in Ireland: When European Law Meets National Recalcitrance. *Data Retention in Europe and Beyond Law and Policy in the Aftermath of an Invalidated Directive*, (Query date: 2026-04-28 17:32:31), 165–180. https://doi.org/10.1093/9780191998980.003.0010

Meireles, A. V. (2024). Digital rights in perspective: The evolution of the debate in the Internet Governance Forum. *Politics and Policy*, *52*(1), 12–32. https://doi.org/10.1111/polp.12571

Mitsilegas, V. (2025). Data Retention and the Judicial Parameters of Mass Surveillance in EU Law. *Data Retention in Europe and Beyond Law and Policy in the Aftermath of an Invalidated Directive*, (Query date: 2026-04-28 17:32:31), 27–44. https://doi.org/10.1093/9780191998980.003.0003

Montasari, R. (2024). Analysing Ethical, Legal, Technical and Operational Challenges of the Application of Machine Learning in Countering Cyber Terrorism. *Advanced Sciences and Technologies for Security Applications*, (Query date: 2026-04-28 17:32:31), 159–197. https://doi.org/10.1007/978-3-031-50454-9_9

Padden, M. (2024). Digitalisation, democracy and the GDPR: The efforts of DPAs to defend democratic principles despite the limitations of the GDPR. *Big Data and Society*, *11*(4). https://doi.org/10.1177/20539517241291815

Panteli, D. (2025). Artificial intelligence in public health: Promises, challenges, and an agenda for policy makers and public health institutions. *Lancet Public Health*, *10*(5). https://doi.org/10.1016/S2468-2667(25)00036-2

Perriello, L. E. (2024). Digital Surveillance Under European Scrutiny. A Dangerous Alliance Unveiled. *Italian Law Journal*, *10*(1), 499–516.

Pesole, A. (2025). Algorithmic Management and the Platformisation of Work in Europe: Evidence from Spain and Germany. *Indian Journal of Labour Economics*, *68*(2), 367–394. https://doi.org/10.1007/s41027-024-00544-y

Powell, M. (2024). Consent, Background Justice and Patterned Privacy Principles. *Political Studies*, *72*(3), 944–960. https://doi.org/10.1177/00323217231167074

Saini, D. (2026). Balancing Safety and Privacy and Necessary Safeguards to Ensure Privacy and Prevent Surveillance. *Journal of Human Rights and Social Work*, (Query date: 2026-04-28 17:32:31). https://doi.org/10.1007/s41134-026-00449-4

Saxena, S. (2025). Balancing Surveillance and Privacy: Analyzing Body-Worn Camera Use by Police in Light of the Digital Personal Data Protection Act, 2023. *Rethinking the Police for A Better Future Navigating Policing Challenges with Accountability and Trust*, (Query date: 2026-04-28 17:32:31), 299–309. https://doi.org/10.1007/978-3-031-83173-7_20

Tampubolon, M. (2025). Cybercrime, Human Rights, and Digital Privacy: Navigating the Complex Landscape of Protection and Freedom. *Studies in Systems Decision and Control*, *608*(Query date: 2026-04-28 17:32:31), 75–85. https://doi.org/10.1007/978-3-031-96641-5_7

Thamer, N. (2025). Cyberattacks on Video Surveillance Systems Challenges and Privacy Issues. *Signals and Communication Technology*, (Query date: 2026-04-28 17:32:31), 21–29. https://doi.org/10.1007/978-3-031-88634-8_3

Ungern-Sternberg, A. v. (2025). Automated law enforcement: Perfect vision or dystopia? *Research Handbook on the Law of Artificial Intelligence Current and Future Directions Second Edition*, (Query date: 2026-04-28 17:32:31), 250–274. https://doi.org/10.4337/9781035316496.00020

Vannini, S. (2024). Drawing a Map in the Sand: Locating an Ethics of Care in the ICT-Related Migration Practices of Older Volunteers in the US Southwest. *IFIP Advances in Information and Communication Technology*, *709*(Query date: 2026-04-28 17:32:31), 205–220. https://doi.org/10.1007/978-3-031-66986-6_16

Yan, M. (2026). Digital innovation and legal protection in China's predictive policing. *Computer Law and Security Review*, *60*(Query date: 2026-04-28 17:32:31). https://doi.org/10.1016/j.clsr.2026.106273

Young, G. W. (2025). Are You Being Played? Video Games as a Lens for Artificial Intelligence Ethics and Data Politics. *Games and Culture*, (Query date: 2026-04-28 17:32:31). https://doi.org/10.1177/15554120251409051

Zahra, A. (2025). Algorithmic Surveillance and the Erosion of Privacy: Reconciling National Security and Human Rights in the Digital Era A Comparative Study of the USA and UAE. *2025 International Conference on Computational Intelligence and Knowledge Economy Iccike 2025*, (Query date: 2026-04-28 17:32:31), 633–638. https://doi.org/10.1109/ICCIKE67021.2025.11318249