

Research Article

Protection of Privacy Rights in The Digital Era Between Cybersecurity and Freedom of Information

Kaaisar Romolus Deo Sianipar ^{1,*}, Rahmayanti Rahmayanti ², Andi Gultom ³

¹ Universitas Pembangunan Panca Budi, Indonesia ; e-mail: kaaisarrdsianipar@gmail.com

² Universitas Pembangunan Panca Budi, Indonesia ; e-mail: rahmayanti@dosen.pancabudi.ac.id

³ Universitas Pembangunan Panca Budi, Indonesia ; e-mail: andigultom1502@gmail.com

Address: Jln. Jend. Gatot Subroto Km. 4.5 Sei Sikambing 20122 Medan City, North Sumatra Province, Indonesia.

* Corresponding Author: Kaaisar Romolus Deo Sianipar

Abstract: The digital era has brought significant changes in the way humans access, store, and share information. Amidst these technological advances, major challenges have emerged to the protection of individual privacy rights. Personal information is increasingly easy to collect and process by various parties, both by state institutions, technology companies, and individual users. On the other hand, the need for freedom of information is also increasing, especially in the context of transparency, public participation, and data openness. The balance between cybersecurity and freedom of information is a crucial issue that must be addressed comprehensively. This paper aims to examine the protection of privacy rights in the digital era by highlighting the tension between data security efforts and demands for information openness. The method used is a literature study with a qualitative approach. The results of the study show that privacy protection requires clear regulations, such as the Personal Data Protection Law in Indonesia, as well as public awareness in protecting personal data. On the other hand, freedom of information must still be maintained so that it is not misused to violate individual rights. Therefore, a balanced approach is needed between regulation, education, and technology to create a digital space that is safe, fair, and respects human rights.

Keywords: cybersecurity, data regulation, digital era, freedom of information, privacy.

1. Introduction

Background

The development of digital technology in the past decade has brought about a major transformation in the lives of the global community. Digitalization creates widespread access to information and enables the rapid exchange of data across geographical boundaries. However, these advancements also present new challenges, especially in relation to personal data protection and individual privacy rights. Personal data is no longer limited to formal identities such as name and address, but also includes digital behavioral preferences, location, and online activity records that can be tracked and monetized by third parties (Pratama & Dewi, 2023).

Society now lives in an increasingly open digital space, where various social media platforms, e-commerce and other digital services require users to share their personal information as a prerequisite for access. This blurs the lines between private and public spaces, increasing the risk of data leakage and misuse. Many users do not have sufficient digital literacy

Received: June 15, 2025;

Revised: June 30, 2025;

Accepted: July 11, 2025;

Published: July 14, 2025

Curr. Ver.: July 14, 2025



Copyright: © 2025 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY SA) license (<https://creativecommons.org/licenses/by-sa/4.0/>)

to understand how their data is used and processed by service providers. Research by Nugraheni and Yuliani (2022) shows that most internet users in Indonesia still lack understanding of the long-term consequences of granting personal data access permissions to applications or digital platforms.

When the right to privacy is not adequately protected, individuals have the potential to become victims of digital crimes such as identity theft, online fraud, and manipulation of data-based algorithms for commercial and political interests. Cybersecurity then becomes an important issue that is directly related to the protection of the right to privacy. Countries around the world, including Indonesia, have responded by drafting a legal framework for personal data protection, as contained in Law No. 27 of 2022 on Personal Data Protection. However, according to Rizky and Astuti (2024), the implementation of this regulation still faces various obstacles, both in terms of digital infrastructure, human resource capacity, and public awareness of the importance of data protection.

The challenge does not stop at security, but also concerns the need for freedom of information. In a democratic state, access to information is a citizen's right to ensure active participation in governance and public decision-making processes. However, freedom of information often clashes with privacy rights, especially in the context of media reporting, journalist investigations, or government data disclosure policies. This situation demands a meeting point between the protection of individual rights and the public interest, so that both values can run harmoniously without negating each other (Wibowo & Lestari, 2023).

The balance between the right to privacy and freedom of information needs to be carefully managed through a multidisciplinary approach that includes legal, ethical, technological, and public education aspects. Government, society and the private sector must collaborate to create a healthy and equitable digital ecosystem. Regulation is not enough, it also requires increased digital awareness and moral responsibility from all parties involved in data processing and dissemination. Privacy protection and information disclosure are not contradictory, but two sides of the same coin in maintaining human dignity and democracy in the digital era.

Problem Formulation

1. What is the form of privacy rights protection in the digital era in the context of cybersecurity?
2. How can freedom of information be aligned with the protection of individual personal data?

2. THEORETICAL STUDY

The right to privacy is a part of human rights that includes an individual's freedom to control their personal data and information. In the digital context, the right to privacy is not

only related to the protection of formal identity, but also includes digital activities, biometric data, and algorithmic preferences that are often collected by online systems. According to Solove (2022), the right to privacy in the digital era should be understood as the right to have an autonomous space from surveillance, intervention, and exploitation of data without valid consent. In Indonesia, the regulation of the right to privacy has begun to be formally strengthened through Law No. 27 of 2022 on Personal Data Protection, which places individual control over their personal data as a key principle.

Cybersecurity conceptually refers to systematic efforts to protect data, networks, and systems from disruptions that can cause both material and non-material losses. According to Hafidz and Ratnasari (2023), cybersecurity includes technical dimensions such as encryption and firewalls, as well as regulatory and educational aspects that involve the role of the state, technology companies, and users. In this perspective, the protection of individual privacy is an integral part of cybersecurity because personal data leaks are often the entry point for digital crimes such as hacking, fraud, and the spread of false information.

Freedom of information, as a democratic principle, guarantees every citizen the right to access, obtain and convey information. This principle is also stipulated in Article 28F of the 1945 Constitution, which guarantees freedom of information as part of freedom of speech. However, this freedom is not without limits, especially when it intersects with the personal rights of individuals. In a study by Putri and Andhika (2023), it is emphasized that proportional restrictions are needed so that freedom of information does not violate one's privacy, especially in the practice of journalism, public investigations, and government data disclosure. Therefore, freedom of information and privacy protection must go hand in hand with the principles of fairness, prudence, and common interest.

3. RESEARCH METHOD

This research uses a descriptive qualitative approach with a library research method. This approach was chosen to explore in depth the phenomenon of privacy rights protection in the digital era which is closely related to legal, social and technological aspects. Data were collected from various secondary sources such as scientific journals, books, laws and regulations, reports of international institutions, and expert opinion articles published within the last three years (2022-2024). The analysis was done thematically by grouping information based on the main issues, namely personal data protection, cybersecurity, and freedom of information.

The validity of the data was strengthened by source triangulation technique, which compares various references that discuss similar issues from different perspectives, including legal, ethical, and public policy perspectives. The data that has been collected is then analyzed using a content analysis model to identify patterns, conflicts, and policy recommendations that

emerge in academic discourse and practice. The aim of this method is to provide a comprehensive picture of how challenges and opportunities in the protection of privacy rights in the digital era can be responded to through fair and effective policies and multidisciplinary approaches.

4. RESULTS AND DISCUSSION

Challenges of Privacy Protection in Cybersecurity

Privacy protection in the digital age faces major challenges due to the increasing complexity of digital systems and the limited control individuals have over the personal data they generate. Big data, artificial intelligence, and internet of things (IoT) technologies allow third parties to collect and analyze large amounts of data, often without the conscious consent of data owners. According to Setyowati and Ramadhan (2023), most internet users do not realize that their online activities are systematically recorded and can be used for commercial, political, or manipulative purposes.

Lack of technical regulation and oversight in data management exacerbates threats to privacy. Many tech companies are not transparent about the purpose and extent of their processing of user data. In Indonesia, despite the enactment of Law No. 27 of 2022 on Personal Data Protection, its implementation is still partial and does not include strong oversight mechanisms. Research by Wahyuni and Hidayat (2024) shows that most companies have not adjusted their privacy policies to the provisions of the PDP Law, especially in terms of explicit consent and user access rights.

Society's dependence on digital services makes personal data a strategic commodity that is vulnerable to misuse. High digital penetration without digital literacy makes it easy for people to provide access to sensitive information without understanding the risks. Data from a survey reviewed by Sari and Nugroho (2022) revealed that 63% of internet users in Indonesia do not read the terms and conditions of digital applications before agreeing to them. This shows that privacy protection is not just about technology, but also about collective awareness and state policy.

Freedom of Information vs Privacy: Two Rights that Must Be Managed

Freedom of information is an important principle in a democratic state that guarantees public access to public information. In the context of government, information disclosure serves as a means of control over the performance of public officials and as a means of citizen participation in policy making. According to Lestari and Firmansyah (2023), the right to information is an integral part of the right to opinion and expression as stipulated in the constitution and international law. Even so, not all information can be accessed freely, as there are ethical and legal restrictions, especially when the information concerns personal data.

Tensions between freedom of information and the right to privacy often occur in journalistic practice and open government. Information disseminated under the pretext of

public interest sometimes violates individual privacy, especially in cases of news involving public figures or crime victims. According to Putra and Salsabila (2024), mass media are often caught in a dilemma between fulfilling the public's right to know and respecting individual rights to personal data protection. In this context, the journalistic code of ethics and data protection regulations must strengthen each other so that there is no violation of either right.

Balanced regulations are needed so that freedom of information and privacy rights do not negate each other. The government must design a clear information classification mechanism and set the boundaries of public interest proportionally. Research by Dewi and Maulana (2022) emphasizes the importance of a normative-progressive approach, where information disclosure is combined with respect for the basic rights of citizens, including privacy. In this way, freedom of information does not turn into a weapon that hurts individual dignity, and privacy is not used as an excuse to cover up abuses of power.

5. CONCLUSION

Conclusion

The right to privacy and freedom of information are two fundamental principles that must be maintained in a balanced manner in the digital age. Privacy protection has become increasingly important due to the widespread collection and processing of personal data by various parties, both the government and the private sector. On the other hand, freedom of information is still needed to ensure transparency, accountability and public participation. The main challenge that arises is how to design regulations, cybersecurity infrastructure, and digital literacy that can guarantee the protection of individual rights without limiting the public's right to obtain information. The imbalance between the two has the potential to create a digital space prone to abuse of power, human rights violations, and unequal control over information.

Suggestions

The government needs to strengthen the implementation of the Personal Data Protection Law by establishing an independent supervisory institution, increasing the capacity of officials, and clarifying sanctions for violators. In addition, educational institutions and the media should play an active role in improving people's digital literacy to better understand the importance of protecting personal data and using information ethically and responsibly. Businesses must also be more transparent in managing user data and adhere to fair data protection principles. Collaboration between the government, private sector and civil society is needed to create a digital space that is safe, inclusive and respects the constitutional rights of all citizens.

References

- [1] R. P. Dewi and D. A. Maulana, "Protection of privacy rights in the era of information disclosure: A study of legal and ethical perspectives," *Journal of Law and Public Policy*, vol. 13, no. 1, pp. 45–59, 2022.
- [2] A. Hafidz and T. Ratnasari, "Cyber security as the foundation of personal data protection in Indonesia," *Journal of Digital Security and Information Technology*, vol. 5, no. 2, pp. 87–101, 2023.
- [3] M. Lestari and B. Firmansyah, "Freedom of information and the ethical challenges of digital journalism," *Journal of Communication and Digital Media*, vol. 8, no. 1, pp. 23–35, 2023.
- [4] R. Nugraheni and T. Yuliani, "Digital literacy and privacy awareness among young internet users," *Journal of Education and Information Technology*, vol. 10, no. 2, pp. 112–125, 2022.
- [5] M. D. Pratama and A. S. Dewi, "The impact of digital technology on personal data privacy: A critical review," *Journal of Digital Social Sciences and Humanities*, vol. 9, no. 3, pp. 203–218, 2023.
- [6] R. A. Putra and N. Salsabila, "Ethical dilemmas in digital media reporting: Between public interest and individual privacy," *Journal of Ethics and Mass Communication*, vol. 6, no. 1, pp. 66–80, 2024.
- [7] F. Rizky and N. P. Astuti, "Implementation of personal data protection law: Between hope and reality," *Indonesian Cyber Law Journal*, vol. 4, no. 1, pp. 14–28, 2024.
- [8] D. A. Sari and H. R. Nugroho, "Digital privacy literacy in the era of big data: A case study of mobile application usage," *Journal of Technology and Digital Society*, vol. 7, no. 2, pp. 93–107, 2022.
- [9] L. Setyowati and T. A. Ramadhan, "Privacy as a constitutional right in the era of information digitalization," *Journal of Law and Constitution*, vol. 12, no. 1, pp. 30–46, 2023.
- [10] A. M. Wahyuni and R. Hidayat, "Company compliance with the personal data protection law in Indonesia: An empirical analysis," *Journal of Information Technology Regulation and Policy*, vol. 5, no. 2, pp. 55–70, 2024.