West Science Law and Human Rights
Vol. 3, No. 03, July 2025, pp. 211~216

The Right to Privacy in International Law: Evolving Standards for Personal Data Protection in the Digital Era

Lutfiah Sholikhatun Nafi'ah[1], Rina Arum Prastyanti[2]
[1,2]Duta Bangsa University

Article Info

Article history:

Received June, 2025
Revised July, 2025
Accepted July, 2025

Keywords:

Human rights;
Security vs privacy;
Privacy;
Personal data protection;
International regulation

ABSTRACT

Privacy and personal data protection are increasingly important issues in today's digital era. This article highlights the importance of recognizing privacy as a fundamental human right that must be protected by the state in accordance with applicable human rights principles and the constitution. Protection of personal data is becoming increasingly crucial because it is often a target for irresponsible parties. International regulations, such as the Universal Declaration of Human Rights and the General Data Protection Regulation (GDPR) in the European Union, provide a framework for the protection of personal data. This article also highlights a key challenge to protecting privacy, namely finding a balance between the need for security and individual privacy. Efforts such as developing specific laws on personal data protection, increasing public awareness, and enhancing international cooperation are urgently needed. Keywords: privacy, data protection, human rights, regulations, challenges.

Corresponding Author:

Name: Lutfiah Sholikhatun Nafi'ah
Institution: Duta Bangsa University
e-mail: lutfiahnafiah2@gmail.com

1. INTRODUCTION

The rapid development of digital technology has revolutionized the way humans interact, work, and access information. In this digital age, personal data is no longer just static information [1], but has become a valuable asset for individuals, corporations, and countries alike [2], [3].

Every online activity, from the use of social media, e-commerce transactions, to participation in government administration systems, generates digital traces that reflect a person's identity, habits, preferences, and even ideological views. Amidst this massive flow of data, serious challenges have emerged to the right to privacy as one of the most fundamental human rights [4], [5].

The right to privacy has increasingly come under scrutiny due to the massive collection, storage, and processing of data by governments and private companies. These activities are often carried out without the explicit consent of the data owners, or even without their understanding of how the data will be used. This raises concerns about data misuse, privacy violations, and disproportionate mass surveillance [6]. Such practices blur the line between public security and personal rights, requiring regulations and legal policies that can address the complexities of the digital age.

Globally, the right to privacy has been recognized in various international legal instruments such as the Universal Declaration

of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). In this context, privacy is not only seen as the right to be free from interference in one's private life, but also includes control over personal information, the right to determine access, and the right to know the purpose of data processing. However, these international legal norms must continue to evolve to keep pace with the dynamics of technology that transcend national jurisdictional boundaries.

A number of new legal principles and standards have emerged amid growing concerns about personal data security. One of these is the General Data Protection Regulation (GDPR), which has been in force in the European Union since 2018. The GDPR explicitly grants individuals the right to control their own data, including the right to access, restrict, correct, and delete personal data held by organizations. This regulation also requires public and private institutions to apply the principles of transparency, accountability, and data protection from the outset (privacy by design) [6]–[9].

In Indonesia, the urgency of personal data protection has begun to receive more attention in recent years, especially after several large-scale data leaks, such as those that occurred in the BPJS Kesehatan, eHAC, and public applications. Although the government has passed Law No. 27 of 2022 on Personal Data Protection (PDP Law), its implementation still faces various challenges such as institutional infrastructure, public awareness, and harmonization with other sectoral regulations. It should be emphasized that the existence of regulations is not the end of the problem, but rather the starting point for systemic transformation in the protection of citizens' digital rights.

The issue of personal data protection is also relevant in the context of globalization and cross-border cooperation. In many cases, personal data of citizens of one country can be accessed, stored, or processed by entities operating in another country. This raises cross-border legal challenges (cross-border data flow) that require a more robust international legal framework and mutual recognition of protection standards. This is where the role of international organizations and multilateral forums is important in promoting collaboration and convergence of personal data protection standards. This research is important to understand the international legal response to digital challenges through the establishment of effective and adaptive data protection standards, as well as to examine the gaps between global norms and local implementation. Apart from legal aspects, personal data protection also concerns ethics and human rights, as privacy reflects individual autonomy in a democratic society.

Its loss can limit freedom of expression and activity. Technological developments such as the IoT, big data, and AI add to the complexity of data management, which without supervision can become a tool for social control. Therefore, a collaborative and balanced legal approach is needed, particularly in responding to the dilemma between national security and privacy protection, so that there is no abuse in the name of public interest.

2. METHODS

This study uses a normative legal approach that focuses on the study of legal norms, both those written in legislation and international legal principles. This approach was chosen because the main issue in this study is closely related to the right to privacy as part of human rights and the framework for personal data protection in international law, which is substantially normative in nature. The primary data sources in this study are secondary data, which include: (1) primary legal materials such as the Universal Declaration of Human Rights (1948), the International Covenant on Civil and Political Rights (1966), the European Convention on Human Rights (1950), the General Data Protection Regulation (GDPR, 2018), as well as Law Number 27 of 2022 concerning Personal Data Protection in Indonesia; (2) secondary legal materials in the form of legal

literature, scientific journals, academic articles, and official reports from international and government institutions; and (3) tertiary legal materials such as legal dictionaries and international legal encyclopedias used to strengthen the understanding of basic concepts [2], [9]–[12].

The analysis in this study was conducted qualitatively by examining legal documents, expert opinions, and relevant legal doctrines through content analysis to understand the substance of personal data protection norms. In addition, a comparative legal approach was used to see how international regulations, particularly the GDPR, can be used as a reference in strengthening the data protection system in Indonesia. The purpose of this method is to gain a comprehensive understanding of the development of data protection standards in international law, identify gaps between global and national regulations, and formulate legal policy recommendations for privacy that are more adaptive to current and future digital challenges.

3. RESULTS AND DISCUSSION

3.1 Evolution of the Concept of Privacy in International Law

The right to privacy has long been recognized as a fundamental human right. In the Universal Declaration of Human Rights (UDHR) of 1948, Article 12 states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence." Although it does not explicitly mention the term "personal data," this declaration serves as an important foundation that human privacy must be protected by law. This principle was further strengthened in the International Covenant on Civil and Political Rights (ICCPR) of 1966 through Article 17, which reaffirms the prohibition of arbitrary interference and guarantees legal protection of privacy. At the regional level, the European Convention on Human Rights (ECHR) in Article 8 explicitly recognizes the right to private life, family, home, and correspondence. This provision serves as an important legal foundation for the development of the General Data Protection Regulation (GDPR) by the European Union in 2018 as a response to the challenges of personal data protection in the digital age.

The right to privacy, previously understood as protection of individuals from arbitrary interference, has evolved into a collective issue in the context of digital technology. Advances in information technology and the widespread practice of surveillance by the state and the private sector have expanded the scope of privacy [13]. This transformation is reflected in the GDPR framework, which builds its foundation on human rights conventions but also addresses modern needs with principles such as the right to be forgotten, informed consent, and data accountability [14]. Privacy is now a structural issue, as digital footprints and massive data processing impact social equality and civil liberties [15]. Uncontrolled digital surveillance has the potential to erode democracy and individual autonomy, necessitating regulations that favor human rights [16]. Invasions of privacy undermine the public interest, affirming that privacy is a common good [17]. Therefore, the GDPR serves as an important legal instrument in building comprehensive data protection that reflects the universal values upheld in democratic societies [14].

3.2 Key Principles of the GDPR and Its Global Impact

The General Data Protection Regulation (GDPR) is the most comprehensive international legal instrument regulating the protection of personal data.

The GDPR introduces fundamental principles such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability. One of the main strengths of the GDPR lies in its extraterritorial nature, whereby its provisions apply not only to organizations operating within the European Union, but also to any entity outside the EU that processes personal data of EU citizens. As

such, the GDPR establishes global jurisdiction over data processing activities, including those conducted online and across borders [18], [19]. The implications of this approach reflect a step forward in international law, particularly in efforts to enforce data protection rights across jurisdictions and overcome domestic legal limitations in guaranteeing the digital rights of citizens.

The impact of the GDPR is felt globally, particularly in Asia and Africa, where many countries are beginning to overhaul their data protection regulatory frameworks to align with GDPR standards. These adjustments are not only aimed at enhancing protection for their citizens but also as a strategic step in maintaining economic and trade relations with the EU [20], [21]. GDPR principles such as transparency, accountability, and fairness are now adopted by a number of countries as a reference in developing their national legal systems. However, the implementation of GDPR outside Europe faces various challenges, mainly due to differences in legal systems and data protection cultures in each country [21]. Despite its complexity, the GDPR framework provides a comprehensive foundation that can be adapted to local contexts and aligns with the European Union's obligations to safeguard the fundamental right to data protection as part of human rights at the international level.

3.3 Privacy Protection Challenges in the Digital Age

Despite regulatory advances such as the GDPR, privacy protection in the digital age continues to face complex and multidimensional challenges. One key issue is the imbalance between the pace of technological development and the formation of laws.

Technologies such as big data analytics, artificial intelligence (AI), and machine learning have surpassed the ability of current regulations to anticipate the risks of data processing [22], [23]. The slow pace of legislation, compared to the dynamics of the technology sector, creates legal loopholes that are exploited by various parties, as demonstrated in the controversy sparked by Edward Snowden regarding mass surveillance [24]. On the other hand, national security is often used by states to expand surveillance practices against citizens. Privacy is often compromised for the sake of security, even without adequate transparency or accountability [24], [25].

In addition to technical and political aspects, challenges also arise from low digital literacy among the public, especially in developing countries such as Indonesia. Many individuals do not understand how their data is collected, used, or even traded, making it difficult to demand legal protection for their personal data [22], [25]. Therefore, increasing public awareness and digital education are crucial steps in strengthening individuals' position as data subjects. Another equally important challenge is the lack of global consensus on the principles of personal data protection. Legal inconsistencies between countries complicate cross-border transactions and make it difficult to enforce laws against international privacy violations [23], [26]. Although regional frameworks such as the GDPR in the European Union and the PIPL in China demonstrate different approaches, uniform global standards have yet to be achieved [22].

3.4 Indonesia's Position in the Global Privacy Regulatory Landscape

Indonesia has officially enacted Law No. 27 of 2022 on Personal Data Protection (PDP Law) as an important step in strengthening its privacy legal framework. The law adopts a number of key principles from the GDPR, such as consent, data minimization, and the right to access and correct personal data. However, the implementation of the PDP Law still faces various obstacles, including the absence of an independent supervisory authority (Data Protection Authority) as a regulator and law enforcer, the unpreparedness of the public and private sectors in developing appropriate internal policies, and the lack of socialization and training for law enforcement officials and electronic system operators. Nevertheless, the existence of this law should be appreciated as

it reflects a paradigm shift from a sectoral approach to a holistic approach to data protection. For the PDP Law to be effective, it needs to be integrated with cybersecurity policies, digital government systems, and institutional reforms that support the comprehensive and sustainable implementation of the right to privacy.

4. CONCLUSION

The right to privacy is a crucial issue in international law in this era of digital connectivity. On the one hand, technological advances support innovation and efficiency, but on the other hand, they increase the risk of privacy violations and data misuse. International legal instruments such as the UDHR, ICCPR, ECHR, and GDPR demonstrate global efforts to establish more comprehensive standards for personal data protection, although there are still gaps in implementation between countries. This study emphasizes the importance of regulations that are adaptive to technology and prioritize the protection of human rights. In Indonesia, Law No. 27 of 2022 on Personal Data Protection is an important first step, but its implementation still requires independent oversight and active public participation. Personal data protection is not merely a technical legal issue, but a tangible manifestation of respect for human dignity. Therefore, global synergy and collective awareness are key to creating a safe and fair digital ecosystem.

REFERENCES

[1] A. R. M. Efendy, "Towards enhanced personal data protection: A novel approach to regulation and practice in Indonesia," *E-Justice J. Law Technol.*, vol. 1, no. 1, pp. 1–15, 2024.

[2] I. Hanafi and A. F. Lubis, "Protection of Privacy and Intellectual Property Rights in Digital Data Management in Indonesia," *Easta J. Law Hum. Rights*, vol. 2, no. 01, pp. 33–40, 2023, doi: 10.58812/eslhr.v2i01.151.

[3] N. Purtova, "The law of everything. Broad concept of personal data and future of EU data protection law," *Law, Innov. Technol.*, vol. 10, no. 1, pp. 40–81, 2018, doi: 10.1080/17579961.2018.1452176.

[4] A. Dalal and R. Roy, "JOURNAL OF BASIC SCIENCE AND ENGINEERING CYBERSECURITY AND PRIVACY : BALANCING SECURITY AND INDIVIDUAL," vol. 18, no. 1, pp. 205–223.

[5] M. Cunningham, "Privacy in the age of the hacker: balancing global privacy and data security law," *Geo. Wash. Int'l L. Rev.*, vol. 44, pp. 643–695, 2012.

[6] U. Sarangi, "Information Economy and Data Protection Laws: A Global Perspective," *Int. J. Bus. Manag. Res.*, vol. 6, no. 2, pp. 15–35, 2018, doi: 10.37391/ijbmr.060203.

[7] A. Mattoo and J. P. Meltzer, "International data flows and privacy: The conflict and its resolution," *J. Int. Econ. Law*, vol. 21, no. 4, pp. 769–789, 2019, doi: 10.1093/jiel/jgy044.

[8] W. B. Chik, "The Singapore personal data protection act and an assessment of future trends in data privacy reform," *Comput. Law Secur. Rev.*, vol. 29, no. 5, pp. 554–575, 2013, doi: 10.1016/j.clsr.2013.07.010.

[9] C. Zhao, X. Yuan, J. Long, L. Jin, and B. Guan, "Chinese stock market Pr ep rin t n ot pe er re v Pr ep rin t n ot pe er re v ed".

[10] T. Streinz, "The Evolution of European Data Law," *Evol. EU Law*, vol. 29, pp. 902–936, 2021, doi: 10.1093/oso/9780192846556.003.0029.

[11] A. Beduschi, "Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations," *Data Policy*, vol. 3, no. 1, 2021, doi: 10.1017/dap.2021.15.

[12] T. D. Oganesian, "The right to privacy and data protection in the information age," *J. Sib. Fed. Univ. - Humanit. Soc. Sci.*, vol. 13, no. 10, pp. 1576–1589, 2020, doi: 10.17516/1997-1370-0664.

[13] O. Diggelmann and M. N. Cleis, "How the right to privacy became a human right," *Hum. Rights Law Rev.*, vol. 14, no. 3, pp. 441–458, 2014.

[14] M. E. Bonfanti, "Il diritto alla protezione dei dati personali nel Patto internazionale sui diritti civili e politici e nella Convenzione europea dei diritti umani: similitudini e difformità di contenuti," *Diritti Um. e Dirit. internazionale 5, 3, 2011*, pp. 437–481, 2011.

[15] D. K. Mohsin, "Right to Privacy in Digital Era," *Available SSRN 3678224*, 2020.

[16] K. P. Humble, "Human rights, international law and the right to privacy," *J. Internet Law*, vol. 23, no. 12, pp. 1–14, 2020.

[17] M.-O. Baumann, "Privatsphäre als ethische und liberale Herausforderungen der digitalen Gesellschaft," *Information-wiss. Prax.*, vol. 67, no. 1, pp. 1–6, 2016.

[18] C. Kuner, "Protecting EU data outside EU borders under the GDPR," *Common Mark. Law Rev.*, vol. 60, no. 1, 2023.

[19] A. Cormack, "An Introduction to the GDPR (v3)," *IDPro Body Knowl.*, vol. 1, no. 5, 2021.

[20] L. A. Bygrave, "Privacy and Data Protection in an International Perspective," 1999.

[21] А. Ю. Чурилов, "Принципы Общего регламента Европейского союза о защите персональных данных (GDPR):

проблемы и перспективы имплементации," *Сибирское юридическое обозрение*, vol. 16, no. 1, pp. 29–35, 2019.
[22] Y. Qu, "Privacy Protection in the Digital Age: Challenges and Strategies," *Trans. Soc. Sci. Educ. Humanit. Res.*, vol. 12, pp. 227–234, 2024, doi: 10.62051/cn9t7b17.
[23] O. Reis, N. E. Eneh, B. Ehimuan, A. Anyanwu, T. Olorunsogo, and T. O. Abrahams, "Privacy law challenges in the digital age: a global review of legislation and enforcement," *Int. J. Appl. Res. Soc. Sci.*, vol. 6, no. 1, pp. 73–88, 2024.
[24] J. Damen, L. Köhler, and S. Woodard, "The human right of privacy in the digital age," Universitätsverlag Potsdam, 2017.
[25] M. Akhlaq, H. A. Jahangir, and H. Khan, "Defending the Right to Privacy in the Digital Age Muhammad Akhlaq1, Hafiz Adil Jahangir2, Dr. Hammadullah Khan3".
[26] U. Chugh, "Ethical Considerations in AI Development: Safeguarding Human Rights and Privacy," *Shodh Sagar J. Artif. Intell. Mach. Learn.*, vol. 1, no. 1, pp. 44–49, 2024.