

Analysis of the Internet of Things (IoT) and Its Impact on Individual Privacy from the Perspective of Indonesian Law

Emmy Febriani Thalib^{1*}; Happy Budyana Sari²; Ni Putu Suci Meinarni³

Institut Bisnis dan Teknologi Indonesia.

*Corresponding Author
Emmy Febriani Thalib

Institut Bisnis dan
Teknologi Indonesia.

Article History

Received: 19.09.2024

Accepted: 15.11.2024

Published: 30.11.2024

Abstract: The Internet of Things (IoT) is a concept in which physical objects such as electronic devices, vehicles, and household appliances are equipped with technology that allows them to connect and exchange data over the internet. Data privacy refers to the right of individuals to control their personal information and ensure that it is not misused or accessed without their consent. In the context of IoT, connected devices continuously collect various personal data from users, such as location, habits, and preferences, which can threaten individual privacy if not properly regulated. In Indonesia, the urgency for appropriate regulations related to data privacy protection in the IoT context is crucial. With the rapid growth of IoT in Indonesia, data privacy protection has become increasingly relevant. Clear and robust regulations are needed to ensure that personal data collected by IoT devices is well protected, preventing misuse and privacy violations. This requires comprehensive legal efforts to address these challenges and safeguard individual privacy rights in the IoT era. This study specifically examines the impact of IoT on users from the perspective of Indonesian law. The research employs a literature study method, reviewing relevant laws and regulations, as well as various scientific articles and books as relevant sources.

Keywords: Internet of Things; Data Privacy; Digital Law; Internet Law; Data Protection.

Cite this article:

Thalib, E.F., Sari, H.B., Meinarni, N.P.S., (2024). Analysis of the Internet of Things (IoT) and Its Impact on Individual Privacy from the Perspective of Indonesian Law. *ISAR Journal of Arts, Humanities and Social Sciences*, 2(11), 153-157.

Introduction

The use of Internet of Things (IoT) technology has rapidly expanded in Indonesia in recent years, covering various aspects of life such as smart homes, transportation, healthcare, and industry. IoT enables devices to connect and communicate through the internet, automatically collecting and sharing data. According to Yasirandi, Lander, Sakinah, and Insan (2020), the adoption of IoT products in Indonesia is driven by the need for efficiency and convenience in daily activities, which has made this technology increasingly popular.

However, alongside this growth, concerns about the security and privacy of personal data collected by IoT devices have also emerged. Each IoT device has the potential to gather personal information from users, ranging from health data, daily habits, to physical location. Hanafi and Lubis (2023) highlight that this data is highly sensitive and, if not properly managed, could be misused by irresponsible parties. Thus, privacy issues become critical within the context of IoT usage. In Indonesia, regulations on personal data protection, such as those set forth in Law No. 27 of 2022 (Law No. 27/2022 on Personal Data Protection), aim to provide a clear legal framework to protect individuals' privacy rights. Marune and Hartanto (2021) note that this regulation is

designed to ensure that every collection, storage, and processing of personal data is conducted in a secure and responsible manner. Nevertheless, challenges arise in the implementation of this regulation, especially in ensuring that all IoT devices comply with established security standards.

One significant challenge is the lack of awareness and understanding among both the public and companies about the importance of personal data protection. Many users are not fully aware of the risks associated with data collection by IoT devices. Additionally, many companies lack the necessary technological infrastructure to adequately safeguard user data. Prabowo, Abdurrohman, and Nuha (2023) point out that without a deep understanding and robust security measures, personal data can easily be exploited by malicious third parties. On the other hand, the complexity of IoT technology itself adds to the regulatory and oversight challenges. With numerous connected devices and the variety of data types collected, setting uniform security standards is challenging. This is exacerbated by the fact that not all IoT devices come equipped with strong security protocols, making them vulnerable to cyber-attacks. Therefore, stringent oversight and high-security standards are essential to protect personal data from growing threats.

In addition to technical challenges, legal aspects also require attention. Law enforcement related to data privacy violations in Indonesia still faces numerous obstacles, including a lack of capacity to monitor and enforce compliance with existing regulations. Marune and Hartanto (2021) highlight that although regulations are in place, their implementation is often inconsistent, reducing the effectiveness of the protection offered by law. Thus, a stronger legal framework and more effective oversight mechanisms are needed to ensure that individuals' privacy rights are well-protected in this digital era.

Literature Review

Previous Research

These studies discuss the legal, ethical, and security aspects related to the use of IoT and its implications for individual privacy.

Table 1: The Previous Research table

NO	TITTLE	SUMMARY
1	The Internet of Things (IoT) and its Impact on Individual Privacy: An Australian Perspective(Caron, Bosua, Maynard, & Ahmad, 2016)	This research explores how Australia's Privacy Principles protect individual privacy concerning data collection through IoT. The study highlights the need for globally standardized IoT laws and examines the security, ethical, and privacy threats posed by modern IoT devices.
2	The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws(Karale, 2021)	This article discusses the security and privacy implications of IoT, including legal regulations governing data and privacy protection, and how these laws apply across public and private sectors.
3	Internet of Things: Security and Privacy Implications(Maras, 2015)	This research addresses the ambivalence in utilizing IoT technology and protecting user rights. The study includes cases from multinationals in the U.S. and Japan, as well as perspectives from Singapore on protecting IoT user rights.
4	Governing the Progress of Internet-of-Things: Ambivalence in the Quest of Technology Exploitation and User Rights Protection(Cheryl, Ng, & Wong, 2021)	This article explores privacy and cybersecurity implications related to autonomous vehicles in smart cities.
5	Autonomous Vehicles for Smart and Sustainable Cities: An In-depth Exploration of Privacy and Cybersecurity Implications(Lim & Taeihagh, 2018)	The research also covers the measures taken by the governments of Singapore and Japan to update privacy laws and ensure data confidentiality.

Privacy in the Digital World

Digital privacy is an individual's right and expectation to keep their personal information and online activities confidential and protected from unauthorized disclosure or misuse. Digital privacy encompasses various aspects, including (DeVries, 2003; Fainmesser, Galeotti, & Momot, 2019):

1. **Personal Data:** Includes information that can be used to identify someone, such as name, address, phone number, email address, and financial information.
2. **Confidentiality of Communications:** Involves protecting the content of personal communications, whether through email, instant messaging, phone calls, or social media.
3. **Digital Footprint:** Refers to data generated from online activities, such as search history, websites visited, and social media activities.
4. **Data Security:** Encompasses protecting data from unauthorized access, identity theft, and data breaches.
5. **Right to Be Forgotten:** The ability for individuals to remove their personal information from the internet or specific digital platforms.

Digital privacy has become increasingly important with the rise of digital technology and the internet, which can collect, store, and analysed vast amounts of data about individuals. Protecting digital privacy requires a comprehensive approach, including laws, cybersecurity policies, and best practices in data management.

Internet of Things

The Internet of Things (IoT) is a network of physical devices connected to the internet, allowing them to collect and exchange data. This concept encompasses everything from smart home devices like thermostats and surveillance cameras to large industrial equipment such as sensors and machinery. IoT leverages various technologies, including sensors, cloud computing, and artificial intelligence, to process and analyze the collected data. IoT devices can communicate with each other and with central systems, enabling automation and increased efficiency in areas such as healthcare, manufacturing, and transportation (Gazis, 2021).

IoT brings numerous benefits, including enhanced efficiency, cost savings, and improved user experiences. However, it also poses challenges, particularly concerning data privacy and security. With the growing number of connected devices and the vast amount of data collected, it is essential to ensure that sensitive information is protected and not misused. Data protection, security standards, and regulations are critical issues in the development and implementation of IoT technology (Madakam, Ramaswamy, & Tripathi, 2015).

Methods

This research will use a normative legal research method. Normative legal research is an approach focused on analyzing the normative or legal aspects within a legal system. This approach explores and interprets existing legal norms, including laws, regulations, and applicable legal principles, to understand how the law is applied in a specific context. In normative legal research, researchers use methods of analysis on legal documents, court decisions, and other legal literature to understand, interpret, and evaluate the relevant legal framework. The primary goal is to

provide a better understanding of existing legal norms and their implications in specific cases or general legal practice.

The research will begin with identifying and reviewing various relevant literature sources, including laws, regulations, academic papers, research reports, and policy documents related to data privacy protection within the context of the Internet of Things (IoT) in Indonesia. The next phase involves the collection and critical analysis of the information found to identify patterns, trends, and gaps in the existing literature. Through this process, the research will provide an in-depth understanding of the legal developments related to data privacy in IoT in Indonesia and explore the challenges, solutions, and research directions that can be pursued to fill existing knowledge gaps.

Result and Discussion

The development of the Internet of Things (IoT) in recent years has shown significant growth across various sectors. According to Hussein (2019), IoT-supporting technology has made substantial advancements, paving the way for new applications in many fields. These developments include improvements in device-to-device communication efficiency, data processing, and system integration. A key development is the emergence of IoT in industries such as healthcare, manufacturing, and logistics, allowing for increased automation and more effective data collection.

In agriculture, IoT has facilitated precision farming, enabling more effective and efficient land management. Kour and Arora (2020) note that IoT technology allows real-time monitoring of soil conditions, moisture levels, and crop nutrient needs. This not only boosts production yields but also reduces excessive resource usage, supporting more sustainable farming practices.

Additionally, Nižetić, Šolić, López-de-Ipiña González-de-Artaza, and Patrono (2020) highlight IoT's role in smart city development. Smart cities use IoT devices to enhance residents' quality of life through efficient energy management, improved traffic control, and enhanced security systems. IoT sensors integrated into city infrastructure enable better monitoring and rapid emergency response. However, despite its many benefits, IoT development also faces challenges, especially concerning data security and privacy. With more connected devices and data collected, ensuring sensitive information is protected from misuse is crucial. Data protection, security standards, and regulation are critical issues in the development and application of IoT technology.

The Internet of Things (IoT) significantly impacts data access and privacy. According to Karale (2021), the continuous advancement of IoT technology introduces substantial security and privacy challenges. IoT devices connected to the internet collect and transmit data, which may include users' personal information. These devices increase privacy violation risks, as collected data can be accessed by third parties or hacked by irresponsible individuals, posing risks to the sensitive data stored in the system.

Furthermore, the use of big data in the IoT ecosystem raises new privacy concerns. Sollins (2019) suggests that the large amounts of data generated by IoT devices require improved management and protection. This data, often containing highly detailed personal information, becomes a prime target for cyber attacks. This issue is compounded by the fact that many IoT devices frequently have low security levels, making them

vulnerable to various security threats, such as hacking and malware.

Lee and Ahmed (2021) emphasize that enhancing security and data protection in IoT applications is essential. They argue that adopting IoT technology without attention to security aspects can lead to serious data breaches. For example, the use of poorly protected sensors and devices can expose user data to attacks. Therefore, the development of robust security protocols and data protection policies is critical to ensuring user privacy remains protected.

Overall, the relationship between IoT and data privacy is complex and requires special attention from technology developers, policymakers, and users. Although IoT offers significant benefits, such as increased efficiency and convenience, data privacy risks cannot be overlooked. Proactive steps are needed to develop stringent security standards and adequate regulations to protect individual privacy in the expanding IoT ecosystem.

Data privacy regulations in Indonesia have significantly evolved, especially with the rising adoption of IoT technology. The primary legal basis governing data privacy is the Personal Data Protection Law (Law No. 27 of 2022), which is designed to protect individuals' rights to their personal data. This law obliges digital service providers and IoT device manufacturers to ensure users' personal data is safeguarded and not misused. In the context of IoT, this means that devices collecting, storing, and transmitting data must have adequate security systems to protect that data from unauthorized access.

Alongside strengthened regulations, the Indonesian government is also implementing additional measures to tighten oversight of personal data usage. According to Suwadi, Ayuningtyas, Septiningrum, and Manthovani (2024), regulations regarding telemedicine, which frequently involves the use of IoT devices for health monitoring, underscore the importance of informed consent and confidentiality of medical data. This shows the government's commitment to addressing privacy issues arising from technological advancements, including in the sensitive healthcare sector.

Aminah and Saksono (2021) note that the biggest challenge in implementing e-government in Indonesia is ensuring data security and privacy. IoT implementation in public infrastructure, such as intelligent transportation systems and public services, requires a clear legal framework to protect citizen data. These policies also require government and private entities to comply with specific security standards, including data encryption and user authentication, to prevent data breaches.

Imdad et al. (2020) highlight that despite efforts to strengthen data security, challenges remain in applying security technologies to IoT devices in Indonesia. Attacks on IoT systems, such as man-in-the-middle (MiM) attacks, could jeopardize user data if security measures are not properly implemented. Consequently, Indonesia continues to enhance regulations and security policies to ensure that IoT technology developments do not threaten individuals' data privacy.

Data privacy regulations in Indonesia have been reinforced with the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law). This law establishes a legal framework for managing personal data, covering essential principles such as legality, transparency, and accountability in personal data processing. The

PDP Law requires data controllers to obtain valid consent from data subjects before collecting, processing, or storing personal data. Additionally, this law grants individuals the right to access, correct, and delete their personal data and demands that data controllers maintain confidentiality and security of managed data.

Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), which has undergone amendments with Law No. 19 of 2016 and a second amendment through Law No. 1 of 2024, regulates various activities related to electronic information and transactions. The ITE Law includes provisions on electronic system security, including prohibitions against unauthorized access, data modification, and dissemination of illegal electronic information. This law also introduces the concepts of electronic signatures and electronic evidence as valid proof in legal proceedings.

Government Regulation No. 82 of 2012 on the Organization of Electronic Systems and Transactions provides additional guidelines for managing electronic systems in Indonesia. This regulation mandates security standards for electronic system providers, including obligations to protect personal data and prevent unauthorized access. Additionally, PP No. 82 of 2012 establishes procedures for security audits and incident management, aimed at ensuring the integrity and reliability of electronic systems used by the public and private sectors.

Law No. 36 of 1999 on Telecommunications focuses on regulating telecommunications services, including using telecommunications infrastructure for data transmission. This law emphasizes the importance of privacy and confidentiality in communication and establishes sanctions for violations of privacy rights in telecommunications. In the context of IoT technology, the Telecommunications Law is relevant because many IoT devices use telecommunications networks to communicate and exchange data. Therefore, the existing regulations in this law also contribute to protecting data transmitted through IoT devices. These regulations reflect Indonesia's commitment to enhancing personal data protection and ensuring that digital technology developments, including IoT, respect individual privacy rights.

Implementing data privacy regulations in IoT usage in Indonesia faces several challenges. One of the primary challenges is the lack of clear and unified standards for security and privacy in the IoT ecosystem. Prabowo et al. (2023) indicate that Indonesia does not yet have a comprehensive reference standard to regulate data privacy implementation in the IoT domain. This creates uncertainty for service providers and users regarding the security measures needed to protect personal data. Additionally, with various IoT devices having different security levels, the risks of data leaks and unauthorized access increase.

Furthermore, the complexity of IoT technology and the limitations of technological infrastructure in Indonesia add to the challenges in implementing data privacy regulations. Yasirandi et al. (2020) note that although there is strong interest in adopting IoT products for smart living, many entities in Indonesia are not technologically prepared to manage data security and privacy aspects effectively. Inadequate infrastructure and limited technical resources hinder the ability to implement necessary security controls, including data encryption and user authentication.

Moreover, Rosadi, Suhardi, and Kristyan (2021) highlight regulatory challenges in the context of smart cities relying on IoT

technology. Large-scale data collection by IoT devices in smart cities raises serious concerns about how this data is used and protected. There is an urgent need for stricter regulations and improved law enforcement to ensure that citizen data collected and processed through IoT in smart city initiatives is protected with high privacy standards. Without strong regulations and effective enforcement, there is a significant risk that citizens' personal data could be misused or stolen, leading to severe consequences for individual privacy and security.

The development and implementation of data privacy regulations in Indonesia, particularly regarding IoT technology usage, are crucial steps to ensuring individual data security and privacy in the digital age. Although challenges in implementing these regulations are significant, with increased awareness, technological infrastructure improvements, and stricter oversight, Indonesia can manage the risks associated with IoT usage. Protecting personal data must be a top priority to support sustainable technology growth and ensure that the privacy rights of individuals are well-protected. Support from all stakeholders, including government, industry, and society, is essential to creating a secure and trusted digital ecosystem in Indonesia.

Conclusion

This research highlights the importance of personal data protection in the digital era, particularly in relation to the use of Internet of Things (IoT) technology in Indonesia. Although regulations like the Personal Data Protection Law (PDP Law) have been established, significant challenges remain in its implementation. These challenges include the lack of clear security standards, limitations in technological infrastructure, and a lack of understanding and awareness among the public and companies about the importance of personal data protection. Additionally, weak law enforcement poses a major obstacle in ensuring compliance with existing regulations. However, with these regulations, Indonesia has demonstrated its commitment to protecting citizens' data privacy amidst the rapid development of digital technology.

References

1. Aminah, S., & Saksono, H. (2021). Digital transformation of the government: A case study in Indonesia. *Jurnal Komunikasi: Malaysian Journal of Communication*, 37(2).
2. Caron, X., Bosua, R., Maynard, S. B., & Ahmad, A. (2016). The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. *Computer Law and Security Review*, 32(1), 4–15. Elsevier Ltd.
3. Cheryl, B. K., Ng, B. K., & Wong, C. Y. (2021). Governing the progress of internet-of-things: Ambivalence in the quest of technology exploitation and user rights protection. *Technology in Society*, 64.
4. DeVries, W. T. (2003). Protecting Privacy in the Digital Age. *Berkeley Technology Law Journal*, 18(1).
5. Dewi Rosadi, S., Suhardi, & Kristyan, S. A. (2021). Data privacy law in the application of smart city in Indonesia. *Corporate Law and Legal System 1 Citation Information*, 24(S4).
6. Fainmesser, I. P., Galeotti, A., & Momot, R. (2019). Digital Privacy. *SSRN Electronic Journal*.

7. Gazis, A. (2021). What is IoT? The Internet of Things explained. *Academia Letters*.
8. Hanafi, I., & Lubis, A. F. (2023). Protection of Privacy and Intellectual Property Rights in Digital Data Management in Indonesia. *The Easta Journal Law and Human Rights*, 2(01), 33–40.
9. Hussein, A. R. H. (2019). Internet of Things (IOT): Research challenges and future applications. *International Journal of Advanced Computer Science and Applications*, 10(6).
10. Imdad, M., Jacob, D. W., Mahdin, H., Baharum, Z., Shaharudin, S. M., & Azmi, M. S. (2020). Internet of things (IoT); security requirements, attacks and counter measures. *Indonesian Journal of Electrical Engineering and Computer Science*, 18(3).
11. Karale, A. (2021). The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. *Internet of Things (Netherlands)*.
12. Kour, V. P., & Arora, S. (2020). Recent Developments of the Internet of Things in Agriculture: A Survey. *IEEE Access*.
13. Lee, C., & Ahmed, G. (2021). Improving IoT Privacy, Data Protection and Security Concerns. *International Journal of Technology, Innovation and Management (IJTIM)*, 1(1).
14. Lim, H. S. M., & Taeihagh, A. (2018). Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications. *Energies*, 11(5).
15. Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications*, 03(05).
16. Maras, M. H. (2015). Internet of things: Security and privacy implications. *International Data Privacy Law*, 5(2).
17. Marune, A. E. M. S., & Hartanto, B. (2021). Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective. *International Journal of Business, Economics, and Social Development*, 2(4), 143–152.
18. Nižetić, S., Šolić, P., López-de-Ipiña González-de-Artaza, D., & Patrono, L. (2020). Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *Journal of Cleaner Production*, 274.
19. Prabowo, S., Abdurrohman, M., & Nuha, H. H. (2023). Internet of Things Security and Privacy Policy: Indonesia Landscape (pp. 201–210).
20. Republik Indonesia. (n.d.). Undang-undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Retrieved August 4, 2024, from <https://peraturan.bpk.go.id/Details/274494/uu-no-1-tahun-2024>
21. Sollins, K. R. (2019). IoT big data security and privacy versus innovation. *IEEE Internet of Things Journal*, 6(2).
22. Suwadi, P., Ayuningtyas, P. W., Septiningrum, S. Y., & Manthovani, R. (2024). Legal comparison of the use of telemedicine between Indonesia and the United States. *International Journal of Human Rights in Healthcare*.
23. Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. (2022). . Indonesia: LN.2022/No.196, TLN No.6820, jdih.setneg.go.id: 34 hlm.
24. Yasirandi, R., Lander, A., Sakinah, H. R., & Insan, I. M. (2020). IoT Products Adoption for Smart Living in Indonesia: Technology Challenges and Prospects. 2020 8th International Conference on Information and Communication Technology, ICoICT 2020.