INTERNATIONAL JOURNAL OF LAW AND SOCIAL DEVELOPMENT

NAWALA

Volume 4, Number 1, 2025

Constitutional Right to Personal Data Protection in the Era of Internet of Everything (IoE)

Siti Mariyam [1]

[1] Universitas 17 Agustus 1945 Semarang, Indonesia

Article history:
Received: January 5, 2025
Revised: February 25, 2025
Accepted: April 27, 2025
Published: June 30, 2025

Keywords:
Constitutional Rights,
Data Regulation,
Digital Privacy,
Internet of Everything,
Personal Data Protection.

Identifier:
Nawala
Page: 37-56
https://nawala.io/index.php/ijlsd

Abstract

The Internet of Everything (IoE) era brought a major transformation in connectivity, integrating humans, processes, data, and physical objects into an interconnected digital ecosystem. These developments, while offering efficiency and innovation, also pose serious challenges related to the protection of personal data as part of citizens' constitutional rights. This literature study aims to analyze the legal framework, technological developments, institutional capacity, and the level of digital literacy of the community in ensuring the protection of personal data in Indonesia. The results of the study show that although Law No. 27 of 2022 provides a strong legal basis, implementation challenges still arise in the form of technology costs, literacy gaps, and cross-sector and cross-border coordination. The application of technologies such as encryption, privacy by design, blockchain, and edge computing is considered to strengthen protection, but requires adaptive regulatory support and multi-stakeholder collaboration. This study recommends a holistic, sustainable, and public awareness-based approach to ensure that personal data protection remains guaranteed amid the acceleration of IoE.

*Corresponding author:
(Siti Mariyam)

1. Introduction

The Internet of Everything (IoE) era has transformed the way humans interact with technology by enabling seamless connectivity among devices, systems, data, and people. As an evolution of the Internet of Things (IoT), IoE encompasses not only the linking of physical objects but also the integration of real-time human activities, data flows, and interactions.[1] With the potential to improve efficiency, productivity, and quality of life, IoE has far-reaching implications for the management and protection of personal data. In this context, personal data is a high-value digital commodity, as well as vulnerable to misuse. In Indonesia, the constitutional basis for personal data protection is grounded in Article 28G paragraph (1) and Article 28H paragraph (4) of the 1945 Constitution, which safeguard individual privacy and property. This right has gained greater significance with the rise of digital technologies that enable large-scale collection, processing, and dissemination of data.[2] Nevertheless, the intricate IoE ecosystem, comprising billions of interconnected devices, heightens the risk of privacy breaches through hacking, unauthorized surveillance, or the use of personal data without proper consent.[3]

---

1 Rakhmadi Rahman, Abdul Khaliq Zulfattah, and Haslinda Haslinda, "Meningkatkan Keamanan Edge Computing Dan Iot Dengan Ubuntu Dari Ancaman Real-Time," *Jurnal Riset Sistem Informasi* 1, no. 4 (2024): 04.

2 Niru Anita Sinaga and Riko Nugraha, "Perspektif Hukum Adat Dalam Konstitusi Hukum Positif Di Indonesia," *Jurnal Ilmiah Hukum Dirgantara* 13, no. 1 (2022): 9.

3 Andrea Sukmadilaga and Sinta Dewi Rosadi, "Upaya Hukum Terhadap Pelanggaran Implementasi Internet Of Things (Iot) Dibidang Pelayanan Kesehatan Menurut Ketentuan Perlindungan Data Pribadi," *Jurnal Suara Keadilan* 21, no. 2 (2020): 209.

Protecting personal data in the IoE era extends beyond legal considerations, encompassing technological, ethical, and cybersecurity dimensions as part of a multidisciplinary challenge. Various studies underline the importance of adaptive regulation to technological developments, considering that the data collection model in IoE is very different from the previous digital era.[4] IoE is no longer just about connecting devices, but building a dynamic data ecosystem that involves direct interaction between humans, machines, and artificial intelligence (AI)-based systems.[5]

Regulations on personal data protection in Indonesia have advanced considerably with the introduction of Law Number 27 of 2022 on Personal Data Protection (PDP Law). This law outlines the rights and duties of data subjects, along with the obligations of data controllers and processors, and is anticipated to serve as the primary framework for safeguarding citizens' constitutional rights in the digital environment. However, in the context of IoE, law enforcement challenges become more complex because they involve cross-jurisdictional data interaction, the existence of smart devices that are difficult to trace, and encryption and anonymization technologies that can make investigations difficult.[6]

---

4 Syarifuddin Syarifuddin, Teresia Din, Tri Andriani, Antonius Rino Vanchapo, Hezron Sabar Rotua Tinambunan, and Dhiraj Kelly Sawlani, "Reformasi Hukum di Era Digital:: Tantangan dan Peluang di Indonesia," *Indonesian Research Journal on Education* 4, no. 4 (2024): 3209.

5 Abeer Iftikhar and Kashif Naseer Qureshi, "*Future Privacy and Trust Challenges for IoE Networks*," In *Cybersecurity Vigilance and Security Engineering of Internet of Everything*, Cham: Springer Nature Switzerland, 2023 : Page.199.

6 Muhammad Ariq Abir Jufri and Akbar Kurnia Putra, "Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi," *Uti Possidetis: Journal of International Law* 2, no. 1 (2021): 41.

Furthermore, the phenomenon of datafication, which refers to the systematic conversion of various human activities and behaviors into digital information, has contributed to an unprecedented surge in the volume of data generated within the IoE ecosystem. This includes data produced by a wide array of interconnected devices, such as smart home sensors that monitor household activities, autonomous vehicles that record and transmit operational and environmental data, and health systems that rely on wearable devices to track physiological and behavioral metrics. The continuous accumulation and transmission of such diverse data not only create new opportunities for innovation and efficiency but also raise significant challenges in terms of managing, securing, and protecting personal information in an increasingly complex digital environment. This process, while offering great opportunities for innovation, at the same time poses a serious risk to individual privacy.[7]

Within the framework of the constitution, the protection of personal data is not just an administrative matter, but part of the fundamental protection of human rights. Given the highly dependent nature of IoE on interoperability and data integration, a responsive legal approach based on the principle of privacy by design is needed. This approach emphasizes the need for privacy protection from the design stage of technological systems and infrastructure, not just as a reactive step after a breach. Therefore, this study aims to comprehensively analyze the constitutional

7 Tamaulina Br Sembiring, Johannes Johny Koynja, Tegen Maharaja, Evy Febryani, and Irsyaf Marsal, "Revolusi Teknologi Dan Tantangan Hukum: Perspektif Privasi Dan Keamanan Data Dalam Era Internet of Things (Iot)," *Jurnal Cahaya Mandalika* 3, no. 2 (2023): 1219.

right to personal data protection in the IoE ecosystem, by reviewing the current literature, national and international legal frameworks, and its implications for privacy protection in the digital age. Using the literature study method, this study seeks to provide a complete picture of the relationship between the development of IoE and the urgency of personal data protection as part of citizens' constitutional rights. This analysis is expected to be an academic contribution in the development of public policies oriented towards security and privacy in the midst of an increasingly massive digital transformation.

2. Literature Review

Studies on the constitutional right to personal data protection in the Internet of Everything (IoE) era indicate a strong link between advances in connectivity technologies and the evolution of privacy regulations. As a concept that merges IoT connectivity with the integration of data, processes, and human interactions, IoE introduces novel legal challenges in the governance and protection of personal information.[8] A number of studies confirm that the constitutional right to privacy in Indonesia has been regulated in Articles 28G and 28H of the 1945 Constitution, but its interpretation and implementation in the digital context requires rapid adaptation.[9] Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) is an important milestone, but the literature shows that this regulation faces obstacles

8 Rakhmadi Rahman, Abdul Khaliq Zulfattah, and Haslinda Haslinda, "Meningkatkan Keamanan Edge Computing Dan Iot Dengan Ubuntu Dari Ancaman Real-Time," *Jurnal Riset Sistem Informasi* 1, no. 4 (2024): 04.

9 Niru Anita Sinaga and Riko Nugraha, "Perspektif Hukum Adat Dalam Konstitusi Hukum Positif Di Indonesia," *Jurnal Ilmiah Hukum Dirgantara* 13, no. 1 (2022): 9.

in cross-border implementation and integration with international standards such as the European Union's General Data Protection Regulation (GDPR).[10] [11]

From a technological perspective, IoE expands the scope of cybersecurity risks, including data leaks, hacking, and massive surveillance by third parties.[12] [13] Several studies underscore that smart devices in the IoE, such as home sensors, connected vehicles, and medical devices, produce highly sensitive data that when misused can have a direct impact on the basic rights of individuals.[14] [15] The privacy by design approach proposed by Cavoukian and adapted in local research[16] emphasizes that privacy protection must be integrated from the technology design stage. This is relevant to the results of international studies showing that IoE systems that implement privacy-based design are more effective at preventing breaches.[17]

---

10 Muhammad Ariq Abir Jufri and Akbar Kurnia Putra, "Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi," *Uti Possidetis: Journal of International Law* 2, no. 1 (2021): 41.

11 Nur Alfiana Alfitri, Rahmawati Rahmawati, and Firmansyah Firmansyah. "Perlindungan terhadap data pribadi di era digital berdasarkan Undang-Undang Nomor 27 Tahun 2022." *Journal Social Society* 4, no. 2 (2024): 92-111.

12 Tamaulina Br Sembiring, Johannes Johny Koynja, Tegen Maharaja, Evy Febryani, and Irsyaf Marsal, "Revolusi Teknologi Dan Tantangan Hukum: Perspektif Privasi Dan Keamanan Data Dalam Era Internet of Things (Iot)," *Jurnal Cahaya Mandalika* 3, no. 2 (2023): 1219.

13 Andrea Sukmadilaga and Sinta Dewi Rosadi, "Upaya Hukum Terhadap Pelanggaran Implementasi Internet Of Things (Iot) Dibidang Pelayanan Kesehatan Menurut Ketentuan Perlindungan Data Pribadi," *Jurnal Suara Keadilan* 21, no. 2 (2020): 209.

14 Abeer Iftikhar and Kashif Naseer Qureshi, "*Future Privacy and Trust Challenges for IoE Networks*," In *Cybersecurity Vigilance and Security Engineering of Internet of Everything*, Cham: Springer Nature Switzerland, 2023 : Page.199.

15 Syarifuddin Syarifuddin, Teresia Din, Tri Andriani, Antonius Rino Vanchapo, Hezron Sabar Rotua Tinambunan, and Dhiraj Kelly Sawlani, "Reformasi Hukum di Era Digital:: Tantangan dan Peluang di Indonesia," *Indonesian Research Journal on Education* 4, no. 4 (2024): 3209.

16 Nur Alfiana Alfitri, Rahmawati Rahmawati, and Firmansyah Firmansyah. "Perlindungan terhadap data pribadi di era digital berdasarkan Undang-Undang Nomor 27 Tahun 2022." *Journal Social Society* 4, no. 2 (2024): 92-111.

17 Loso Judijanto, Arief Fahmi Lubis, Donny Eddy Sam Karauwan, Sator Sapan Bungin, and Hedwig Adianto Mau. "Efektivitas Kebijakan Perlindungan Data Pribadi dalam Menjaga Hak Asasi Manusia di Era Teknologi di Indonesia." *Sanskara Hukum dan HAM* 3, no. 01 (2024): 34-42.

In addition, the literature also highlights the importance of public awareness and digital literacy as part of personal data protection. A study by Xanderina et al.[18] found that users' low understanding of digital privacy rights in Indonesia exacerbates the risk of data exploitation. In line with that, research by Dinda (2024) emphasizes the need for synergy between law enforcement, public education, and security technology innovation. Overall, previous studies indicate that the challenge of personal data protection in the IoE era requires a multidimensional strategy: strengthening the legal framework, developing security technologies, and improving digital literacy. The gap between technological developments and regulatory capacity is a crucial issue that must be addressed to ensure citizens' constitutional rights in the digital realm.

3. Method

This study uses a literature review method to examine the constitutional right to personal data protection in the context of the development of the Internet of Everything (IoE). This method was chosen because it allows researchers to integrate findings from various recent academic sources to build a comprehensive and evidence-based understanding. The research process begins with the identification of relevant keywords, such as "personal data protection", "constitutional rights", "Internet of Everything", "IoT and privacy", and "data protection regulations". Searches were conducted on the academic databases Google Scholar to ensure

18 Meilinda Xanderina, Maria Ramanda Kalawa Putri, and Jadiaman Parhusip, "Peran Etika dalam Pencegahan Penyalahgunaan Teknologi Informasi pada Media Sosial," *Jurnal Ilmiah Informatika dan Komputer* 1, no. 2 (2024): 213.

relevance and actuality. From the initial search results, 52 articles were obtained, then selected based on inclusion criteria, namely: (1) discussing the protection of personal data in a legal or technological framework, (2) relevant to the context of IoE or the development of connectivity technology, (3) having peer review or scientific publication status.

These articles cover constitutional law perspectives form Sinaga and Nugraha, aspects of security technology form Nirwan and Sampurna, Iftikhar and Qureshi, as well as multidisciplinary studies that combine legal, technological, and social approaches form Junaedi, dan Xanderina et al. The literature analysis process was carried out using thematic analysis techniques, which focused on grouping issues into three main themes: (1) the constitutional foundation of personal data protection, (2) the challenges of privacy protection in the IoE era, and (3) technology-based data protection strategies and policies. The next stage is data synthesis, which is integrating findings from various sources to produce a consistent and mutually supportive narrative. In this stage, the differences of views between authors are analyzed to provide a comprehensive picture of the variations in approaches. For example, some studies emphasize strengthening legal instruments as a priority,[19] while others highlight the importance of cybersecurity technology and public education (Dinda, 2024).

This method also refers to the principle of critical review, which not only summarizes the content of previous research, but also evaluates its relevance,

19 Muhammad Ariq Abir Jufri and Akbar Kurnia Putra, "Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi," *Uti Possidetis: Journal of International Law* 2, no. 1 (2021): 41.

validity, and limitations. This is important considering that the rapid development of IoE can cause research results to become obsolete if they are not critically analyzed in the current context. With this systematic literature review approach, the research is expected to present a comprehensive and up-to-date review of the constitutional right to personal data protection in the IoE era, as well as provide a conceptual basis for further research or public policy development.

4. Results

4.1. Constitutional Basis for Personal Data Protection in Indonesia

The protection of personal data in Indonesia is firmly grounded in the Constitution, particularly in Article 28G paragraph (1) of the 1945 Constitution, which ensures every individual's right to security and safeguarding themselves, their family, honor, dignity, and property. Furthermore, Article 28H paragraph (4) guarantees everyone's right to possess and maintain their property. In the digital age, these provisions are understood to encompass the right of individuals to manage and control their personal information.[20]

Law No. 27 of 2022 on Personal Data Protection (PDP Law) serves as a dedicated legal framework that reinforces the safeguarding of personal data. This law defines what constitutes personal data, classifies it into general and sensitive categories, and outlines the rights of data subjects, such as the right to receive information, access their data, request corrections, demand deletion, and object to

20 Niru Anita Sinaga and Riko Nugraha, "Perspektif Hukum Adat Dalam Konstitusi Hukum Positif Di Indonesia," *Jurnal Ilmiah Hukum Dirgantara* 13, no. 1 (2022): 9.

the processing of their data.[21] The existence of the PDP Law puts Indonesia in an equal position with countries that have adopted modern legal frameworks such as the European Union's GDPR, although there are still gaps in terms of cross-jurisdictional enforcement and compliance.[22]

In the context of the Internet of Everything (IoE), the protection of personal data is gaining a new dimension. IoE not only connects devices (Internet of Things), but also integrates people, data, processes, and physical objects into one massive digital ecosystem. This increases the potential for real-time and massive data collection, so that the risk of privacy rights violations increases.[23] A study by Sembiring et al.[24] shows that IoE has the potential to blur the line between personal and public data, as much data is generated automatically by smart devices without direct interaction from users. This raises legal challenges related to the validity of consent in data processing.

From a law enforcement perspective, although the PDP Law has regulated administrative and criminal sanctions, the literature confirms that supervision and dispute resolution mechanisms still need to be strengthened (Dinda, 2024). Some

---

21 Nur Alfiana Alfitri, Rahmawati Rahmawati, and Firmansyah Firmansyah. "Perlindungan terhadap data pribadi di era digital berdasarkan Undang-Undang Nomor 27 Tahun 2022." *Journal Social Society* 4, no. 2 (2024): 92-111.

22 Muhammad Ariq Abir Jufri and Akbar Kurnia Putra, "Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi," *Uti Possidetis: Journal of International Law* 2, no. 1 (2021): 41.

23 Andrea Sukmadilaga and Sinta Dewi Rosadi, "Upaya Hukum Terhadap Pelanggaran Implementasi Internet Of Things (Iot) Dibidang Pelayanan Kesehatan Menurut Ketentuan Perlindungan Data Pribadi," *Jurnal Suara Keadilan* 21, no. 2 (2020): 209.

24 Tamaulina Br Sembiring, Johannes Johny Koynja, Tegen Maharaja, Evy Febryani, and Irsyaf Marsal, "Revolusi Teknologi Dan Tantangan Hukum: Perspektif Privasi Dan Keamanan Data Dalam Era Internet of Things (Iot)," *Jurnal Cahaya Mandalika* 3, no. 2 (2023): 1219.

studies recommend the establishment of an independent data protection authority that has full authority to crack down on breaches, similar to Data Protection Authorities in other countries.[25] Thus, a constitutional and specific regulatory foundation is in place, but the challenge lies in adapting and enforcing that is responsive to technological developments such as IoE. Without strengthening legal and institutional capacity, the constitutional right to personal data protection risks being eroded by technological innovations that move much faster than regulations.

4.2. Challenges of Personal Data Protection in the Internet of Everything (IoE) Era

The Internet of Everything (IoE) era brings huge opportunities in connectivity, efficiency, and innovation, but it also creates complex challenges in personal data protection. These challenges are multidimensional, covering technical, legal, and ethical aspects. On the technical side, IoE involves the integration of millions of smart devices, sensors, and artificial intelligence-based systems that collect data in real-time. According to the research of Sukmadilaga & Rosadi,[26] increasing the number of endpoints exponentially expands the attack surface and increases the risk of data leakage. IoE devices often have limited computing

25 Abeer Iftikhar and Kashif Naseer Qureshi, "*Future Privacy and Trust Challenges for IoE Networks*," In *Cybersecurity Vigilance and Security Engineering of Internet of Everything*, Cham: Springer Nature Switzerland, 2023 : Page.197.

26 Andrea Sukmadilaga and Sinta Dewi Rosadi, "Upaya Hukum Terhadap Pelanggaran Implementasi Internet Of Things (Iot) Dibidang Pelayanan Kesehatan Menurut Ketentuan Perlindungan Data Pribadi," *Jurnal Suara Keadilan* 21, no. 2 (2020): 209.

capabilities so they cannot support complex encryption or authentication algorithms, making them vulnerable to hacking.

Legally, the main problem is the speed of technological innovation that exceeds the speed of regulatory adaptation. Law No. 27 of 2022 on Personal Data Protection has indeed taken a step forward, but it has not explicitly accommodated the unique characteristics of IoE, such as data collection without direct interaction, cross-border processing, and data ownership generated by automated device interactions.[27] Xanderina et al.[28] emphasize that weaknesses in the harmonization of international law result in difficulties in enforcement, especially when data moves to jurisdictions that have lower standards of protection.

Ethical challenges are no less significant. IoE raises questions about actual informed consent, as users often do not fully understand how their data is collected, analyzed, and used.[29] Many users automatically agree to the terms of service without reading them, so that the agreement becomes a formality that loses substantial meaning. In addition, the issue of algorithm transparency is a concern. IoE devices often rely on machine learning to make decisions, but this decision-making process

---

27 Nur Alfiana Alfitri, Rahmawati Rahmawati, and Firmansyah Firmansyah. "Perlindungan terhadap data pribadi di era digital berdasarkan Undang-Undang Nomor 27 Tahun 2022." *Journal Social Society* 4, no. 2 (2024): 92-111.

28 Meilinda Xanderina, Maria Ramanda Kalawa Putri, and Jadiaman Parhusip, "Peran Etika dalam Pencegahan Penyalahgunaan Teknologi Informasi pada Media Sosial," *Jurnal Ilmiah Informatika dan Komputer* 1, no. 2 (2024): 213.

29 Tamaulina Br Sembiring, Johannes Johny Koynja, Tegen Maharaja, Evy Febryani, and Irsyaf Marsal, "Revolusi Teknologi Dan Tantangan Hukum: Perspektif Privasi Dan Keamanan Data Dalam Era Internet of Things (Iot)," *Jurnal Cahaya Mandalika* 3, no. 2 (2023): 1219.

is often a black box. This makes it difficult for individuals to assess whether their privacy rights have been violated.[30]

The literature also identifies institutional challenges, especially related to the limitations of human and technological resources in supervisory institutions (Dinda, 2024). Without adequate supervisory capacity, regulation will only become the norm without coercion. Thus, the challenges of personal data protection in the IoE era are not only related to technical security loopholes, but also include global legal dynamics, ethical complexities, and institutional limitations. This shows the need for a multidisciplinary approach that combines technology, public policy, and people's digital literacy to ensure the sustainability of the constitutional right to personal data protection.

4.3. Personal Data Protection Strategy in the Internet of Everything (IoE) Era

Personal data protection in the Internet of Everything (IoE) era requires a comprehensive strategy that combines legal, technological, institutional, and public literacy aspects. These strategies must be designed adaptively to deal with the dynamic, distributed, and cross-border nature of IoE. From a legal perspective, strengthening regulations is a priority. Law No. 27 of 2022 concerning Personal Data Protection needs to be harmonized with sectoral regulations such as the ITE Law and Financial Services Authority (OJK) regulations to avoid overlaps and legal

30 Abeer Iftikhar and Kashif Naseer Qureshi, "*Future Privacy and Trust Challenges for IoE Networks*," In *Cybersecurity Vigilance and Security Engineering of Internet of Everything*, Cham: Springer Nature Switzerland, 2023 : Page.198.

loopholes.[31] In addition, it is necessary to establish a Data Protection Authority that is independent, authorized, and has adequate resources to supervise, enforce the law, and educate the public.[32] Harmonization with international standards such as the General Data Protection Regulation (GDPR) can also strengthen protection in the global realm.[33]

Technically, the application of the principles of privacy by design and privacy by default is key. IoE devices must be designed with built-in security mechanisms such as end-to-end encryption, multi-factor authentication, and strong digital identity management.[34] The use of blockchain for recording data transactions can provide transparency and minimize the risk of data manipulation.[35] Additionally, edge computing can be used to process data near the source, thereby reducing the need for the transfer of raw data to the center, potentially lowering the risk of leakage.[36] The institutional approach is no less important. Supervisory institutions require human resources with technical expertise in the fields of cybersecurity,

---

31 Nur Alfiana Alfitri, Rahmawati Rahmawati, and Firmansyah Firmansyah. "Perlindungan terhadap data pribadi di era digital berdasarkan Undang-Undang Nomor 27 Tahun 2022." *Journal Social Society* 4, no. 2 (2024): 92-111.

32 Abeer Iftikhar and Kashif Naseer Qureshi, "*Future Privacy and Trust Challenges for IoE Networks*," In *Cybersecurity Vigilance and Security Engineering of Internet of Everything*, Cham: Springer Nature Switzerland, 2023 : Page.199.

33 Muhammad Ariq Abir Jufri and Akbar Kurnia Putra, "Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi," *Uti Possidetis: Journal of International Law* 2, no. 1 (2021): 41.

34 Andrea Sukmadilaga and Sinta Dewi Rosadi, "Upaya Hukum Terhadap Pelanggaran Implementasi Internet Of Things (Iot) Dibidang Pelayanan Kesehatan Menurut Ketentuan Perlindungan Data Pribadi," *Jurnal Suara Keadilan* 21, no. 2 (2020): 209.

35 Tamaulina Br Sembiring, Johannes Johny Koynja, Tegen Maharaja, Evy Febryani, and Irsyaf Marsal, "Revolusi Teknologi Dan Tantangan Hukum: Perspektif Privasi Dan Keamanan Data Dalam Era Internet of Things (Iot)," *Jurnal Cahaya Mandalika* 3, no. 2 (2023): 1219.

36 Rakhmadi Rahman, Abdul Khaliq Zulfattah, and Haslinda Haslinda, "Meningkatkan Keamanan Edge Computing Dan Iot Dengan Ubuntu Dari Ancaman Real-Time," *Jurnal Riset Sistem Informasi* 1, no. 4 (2024): 04.

technology law, and digital forensics (Dinda, 2024). Cross-sectoral cooperation between government, industry, academia, and civil society needs to be built through national coordination forums.

In terms of public literacy, the strategy must include public education about privacy rights, data protection techniques, and awareness of digital threats. Digital literacy campaigns can utilize social media, online education platforms, and collaborations with schools and universities.[37] Finally, this strategy should be dynamic and responsive. Periodic evaluations of regulations and technologies need to be conducted to adapt to new trends, such as the integration of IoE with generative artificial intelligence, digital twins, and quantum computing, which have the potential to drastically change the privacy threat landscape. With the implementation of this comprehensive strategy, the constitutional right to personal data protection can be maintained amid the acceleration of IoE development.

5. Discussion

Protecting personal data in the Internet of Everything (IoE) era requires a far more intricate approach compared to the traditional internet era. Literature reviews indicate that the challenges extend beyond technical issues, encompassing legal, ethical, and institutional dimensions as well. Addressing these challenges necessitates a combination of robust regulations, technological advancements, and active public engagement. Legally, Law No. 27 of 2022 on Personal Data Protection represents a

37 Meilinda Xanderina, Maria Ramanda Kalawa Putri, and Jadiaman Parhusip, "Peran Etika dalam Pencegahan Penyalahgunaan Teknologi Informasi pada Media Sosial," *Jurnal Ilmiah Informatika dan Komputer* 1, no. 2 (2024): 213.

significant step in upholding citizens' constitutional right to privacy. However, the development of cross-border IoE technology has raised the problem of jurisdiction gap, namely differences in data protection standards and rules between countries.[38] Without effective international cooperation mechanisms, law enforcement will be difficult, especially for breaches involving cloud servers or service providers abroad. From a technical aspect, the increasing number of connected devices in IoE increases the risk of data leakage.

Privacy by design approaches and technologies such as encryption, blockchain, and edge computing can be solutions, but their application is still limited due to cost factors, device limitations, and lack of standardization.[39] This means that technical solutions cannot stand on their own without the support of policies and regulations that drive industry compliance. The ethical dimension becomes important when discussing informed consent in IoE. Research by Sembiring et al.[40] shows that most users give consent without understanding the implications. This indicates the asymmetry of information between the service provider and the user, which in turn weakens the individual's control over his or her personal data. Institutions also play a vital role. Supervisory institutions need to have adequate

38 Muhammad Ariq Abir Jufri and Akbar Kurnia Putra, "Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi," *Uti Possidetis: Journal of International Law* 2, no. 1 (2021): 41.

39 Andrea Sukmadilaga and Sinta Dewi Rosadi, "Upaya Hukum Terhadap Pelanggaran Implementasi Internet Of Things (Iot) Dibidang Pelayanan Kesehatan Menurut Ketentuan Perlindungan Data Pribadi," *Jurnal Suara Keadilan* 21, no. 2 (2020): 209.

40 Tamaulina Br Sembiring, Johannes Johny Koynja, Tegen Maharaja, Evy Febryani, and Irsyaf Marsal, "Revolusi Teknologi Dan Tantangan Hukum: Perspektif Privasi Dan Keamanan Data Dalam Era Internet of Things (Iot)," *Jurnal Cahaya Mandalika* 3, no. 2 (2023): 1219.

technical capacity, authority, and resources. Without it, regulations will be difficult to enforce.

The European Union's experience in implementing the GDPR shows that the success of personal data protection depends not only on regulation, but also on the effectiveness of surveillance and the level of public literacy. In addition, digital literacy is a foundation that cannot be ignored. The level of public awareness of the right to privacy is still low, so it is vulnerable to being used by irresponsible parties. Massive public education can be a long-term strategy to create a safe and ethical digital ecosystem. Thus, this discussion underscores that the protection of personal data in the IoE era requires multi-faceted integration: adaptive regulation, secure technology, effective enforcement mechanisms, and strong public literacy. Without cross-sectoral and cross-country collaboration, it will be difficult to fully guarantee the constitutional right to personal data protection.

6. Conclusion

The protection of personal data in the Internet of Everything (IoE) era is an integral part of citizens' constitutional rights recognized within the national legal framework. The complexity of the IoE ecosystem, involving billions of connected devices, poses new challenges for data privacy, security, and sovereignty. Based on literature studies, this protection requires a holistic approach that combines legal, technological, institutional, and community literacy aspects. Legally, the existence of Law No. 27 of 2022 is an important foundation, but it requires harmonization with sectoral regulations and international standards.

From a technical perspective, the application of the principles of privacy by design, encryption technology, blockchain, and edge computing can strengthen data security, although the implementation still faces cost and standardization constraints. Institutional capacity, cross-sector collaboration, and increasing public digital literacy are key factors for the success of personal data protection. Without this combination, regulations will be difficult to implement effectively. Therefore, in the midst of accelerating the adoption of IoE, an adaptive, sustainable, and cross-border personal data protection strategy is needed, in order to ensure the constitutional rights of the entire community in the increasingly connected digital era.

References

Alfitri, Nur Alfiana, Rahmawati Rahmawati, and Firmansyah Firmansyah. "Perlindungan terhadap data pribadi di era digital berdasarkan Undang-Undang Nomor 27 Tahun 2022." *Journal Social Society* 4, no. 2 (2024): 92-111.

Iftikhar, Abeer, and Kashif Naseer Qureshi. "*Future Privacy and Trust Challenges for IoE Networks*." In *Cybersecurity Vigilance and Security Engineering of Internet of Everything*, Cham: Springer Nature Switzerland, 2023 : 193-218.

Judijanto, Loso, Arief Fahmi Lubis, Donny Eddy Sam Karauwan, Sator Sapan Bungin, and Hedwig Adianto Mau. "Efektivitas Kebijakan Perlindungan Data Pribadi dalam Menjaga Hak Asasi Manusia di Era Teknologi di Indonesia." *Sanskara Hukum dan HAM* 3, no. 01 (2024): 34-42.

Jufri, Muhammad Ariq Abir, and Akbar Kurnia Putra. "Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi." *Uti Possidetis: Journal of International Law* 2, no. 1 (2021): 31-57.

Rahman, Rakhmadi, Abdul Khaliq Zulfattah, and Haslinda Haslinda. "Meningkatkan Keamanan Edge Computing Dan Iot Dengan Ubuntu Dari Ancaman Real-Time." *Jurnal Riset Sistem Informasi* 1, no. 4 (2024): 01-07.

Sembiring, Tamaulina Br, Johannes Johny Koynja, Tegen Maharaja, Evy Febryani, and Irsyaf Marsal. "Revolusi Teknologi Dan Tantangan Hukum: Perspektif Privasi Dan Keamanan Data Dalam Era Internet of Things (Iot)." *Jurnal Cahaya Mandalika* 3, no. 2 (2023): 1217-1222.

Sinaga, Niru Anita, and Riko Nugraha. "Perspektif Hukum Adat Dalam Konstitusi Hukum Positif Di Indonesia." *Jurnal Ilmiah Hukum Dirgantara* 13, no. 1 (2022): 1-19.

Sukmadilaga, Andrea, and Sinta Dewi Rosadi. "Upaya Hukum Terhadap Pelanggaran Implementasi Internet Of Things (Iot) Dibidang Pelayanan Kesehatan Menurut Ketentuan Perlindungan Data Pribadi." *Jurnal Suara Keadilan* 21, no. 2 (2020): 205-221.

Syarifuddin, Syarifuddin, Teresia Din, Tri Andriani, Antonius Rino Vanchapo, Hezron Sabar Rotua Tinambunan, and Dhiraj Kelly Sawlani. "Reformasi Hukum di Era Digital:: Tantangan dan Peluang di Indonesia." *Indonesian Research Journal on Education* 4, no. 4 (2024): 3206-3215.

Xanderina, Meilinda, Maria Ramanda Kalawa Putri, and Jadiaman Parhusip. "Peran Etika dalam Pencegahan Penyalahgunaan Teknologi Informasi pada Media Sosial." *Jurnal Ilmiah Informatika dan Komputer* 1, no. 2 (2024): 211-217.