Journal of Sustainable Development Science
Vol. 7, No. 2, December 2025, pp. 99-106
e-ISSN: 2715-9140 **|** p-ISSN: 2722-919X

Legal Settings About Cyber Security in the Era of Globalization

Anak Agung Sagung Erry Erdyawathy [1*], Cokorde Istri Dian Laksmi Dewi [2], Benyamin Tungga [3]
[1] Ngurah Rai University, Denpasar, Indonesia
[2] Ngurah Rai University, Denpasar, Indonesia
[3] Ngurah Rai University, Denpasar, Indonesia
[1]Email: erry5103@gmail.com
[2]Email: cokdild@gmail.com
[3]Email: benyamintungga18@gmail.com

ABSTRACT

The rapid development of information technology in the era of globalization has created a digital space that not only facilitates cross-country interactions, but also presents various serious threats to cybersecurity and human rights protection. Transnational cyber attacks, personal data breaches, and misuse of digital space are new challenges that require adaptive, comprehensive legal responses that are oriented towards protecting citizens' rights. This study aims to analyze how Indonesia's current legal regulations regulate cybersecurity in facing the challenges of globalization, and how to improve the effectiveness of its regulations in ensuring protection of human rights and privacy. The method used is normative legal research, with a legislative and conceptual approach. The results of the study show that Indonesia already has a number of legal instruments that regulate cybersecurity issues, such as the ITE Law, the PDP Law, and the role of the National Cyber and Crypto Agency (BSSN). However, these regulations are still fragmented and inadequate in dealing with complex and cross-border global threats. In addition, protection of human rights, especially the right to privacy and freedom of expression, has not been fully guaranteed effectively in practice. The conclusion of this study confirms that Indonesia needs legal reform through the establishment of a special law on cybersecurity that is comprehensive and has a human rights perspective. In addition, strengthening inter-agency coordination, establishing an independent supervisory authority, and increasing international cooperation are important steps to build a strong and democratic cybersecurity system in the global era.

Keywords: *Cyber Security, Cyber Law, Digital Privacy, Globalization, Human Rights, UU PDP, UU ITE*

*Corresponding Author:
E-mail: erry5103@gmail.com (Anak Agung Sagung Erry Erdyawathy)
Ngurah Rai University, Denpasar, Indonesia

1. INTRODUCTION

Globalization has transformed the world order towards almost limitless connectivity, accelerating the integration of economic, political, social, and technological systems between countries. In this context, the development of information and communication technology is the main foundation that supports the dynamics of globalization. The digitalization era has created virtual space or cyberspace as the main medium for human interaction across national borders. Howe-ver, behind these extraordinary benefits, serious threats have also emerged in the form of disruptions and cyber attacks (cyber threats) that are not only individual or sectoral in nature, but also threaten national security and global stability. (Judijanto & Nugroho, 2025)

Cybersecurity is a contemporary issue that is increasingly urgent to be regulated

Journal of Sustainable Development Science
Vol. 7, No. 2, December 2025, pp. 99-106
e-ISSN: 2715-9140 **|** p-ISSN: 2722-919X

systematically and comprehensively, considering the high escalation of cybercrime, hacking of critical infrastructure, spread of disinformation, breaches of personal data, and cyber attacks by state actors (state-sponsored cyberattacks). (Budhijanto, 2024)

In recent years, the world has faced an escalating surge in increasingly complex and structured cybercrime. According to the Global Cybercrime Report 2025, economic losses due to global cybercrime are estimated to have reached USD 9.22 trillion in 2024 and are projected to continue to increase to USD 13.82 trillion in 2028. (Jennings-Trace, 2025) This phenomenon reflects changes in digital threat patterns, where perpetrators are no longer limited to individuals or criminal groups alone, but also involve state actors with strategic interests.

One of the most worrying forms of cyberattacks is hacking of critical infrastructure. In this sector, Advanced Persistent Threats (APT) attacks increased by 58% throughout 2024, targeting many public services, energy, telecommunications, and financial sectors. Real examples include the attack on the Ukrainian power grid in 2015 which resulted in power outages for more than 230,000 people, and the cyberattack on the Kyivstar telecommunications system in Ukraine in 2023 which caused losses of up to USD 90 million. (Reuters, 2024)

The phenomenon of personal data breaches also continues to increase significantly. Throughout 2023, more than 33 billion user accounts were exposed due to digital security breaches. In 2024 alone, more than 6.4 billion personal data were reported to have been leaked through various digital attacks, ranging from phishing to ransomware. Phishing attacks now account for around 41% of total data breaches, with losses per incident estimated at USD 4.5 to 5 million. (Reuters, 2024)

Disinformation and deepfakes are also becoming new tools in socio-political conflicts and manipulation. AI-based disinformation campaigns are being used massively in geopolitical conflicts, such as between Iran and Israel, as well as in the spread of domestic hoaxes in various countries. In 2024, there were more than 105,000 cases of deepfakes being used to deceive banking systems and the public, with the impact becoming increasingly difficult to contain. (Klepper, 2025)

More worryingly, cyberattacks are no longer just criminal in nature, but have also become part of a country's military and political strategy. State-sponsored cyberattacks have increased dramatically, with more than 800 major incidents recorded in 2024. Countries such as Russia, Iran, and China are reported to be actively using APT networks to infiltrate other countries' systems, whether for sabotage, strategic data theft, or the spread of disinformation. Collaboration between state actors and cybercriminal groups is increasingly difficult to distinguish, creating a hybrid threat landscape that is difficult to counter conventionally. (Sodiq et al., 2024)

These phenomena are not only technical in nature, but also have complex legal, political, and human rights dimensions. In the Indonesian national legal system, various laws and regulations have been drafted to anticipate these challenges, including through Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) and its amendments, Law Number 27 of 2022 concerning Personal Data Protection (PDP), and the establishment of the National Cyber and

Journal of Sustainable Development Science
Vol. 7, No. 2, December 2025, pp. 99-106
e-ISSN: 2715-9140 | p-ISSN: 2722-919X

Crypto Agency (BSSN) as the main institution managing national cybersecurity.

However, in the midst of the rapid flow of globalization, national legal regulations often experience gaps with practical needs enforcement against perpetrators outside the country's territory, weak international cooperation, and the absence of a comprehensive binding international legal instrument related to cybersecurity. (Novita et al., 2024) This condition is exacerbated by the low digital literacy of the community, inconsistent law enforcement in the country, and overlapping sectoral regulations that weaken the effectiveness of the cybersecurity protection system in Indonesia.

In addition to technical and legal aspects, cybersecurity challenges are also closely related to the protection of human rights, especially the right to privacy, freedom of expression, and access to accurate information. On the one hand, the state has an obligation to guarantee national security and public order in the digital space, but on the other hand it must continue to uphold the principles of democracy and individual rights in the digital era. The tension between the principles of security and freedom is one of the main problems in the formulation and implementation of cybersecurity regulations in various countries, including Indonesia. (Tobing et al., 2024)

Considering this complexity, it is important to comprehensively examine how the legal regulation on cybersecurity in Indonesia responds to the multidimensional challenges of globalization, and how to increase its effectiveness so that it is not only able to answer security issues, but also in line with the principles of democratic and equitable internet governance. This study is expected to contribute to the formation of a national legal system that is adaptive to technological developments, responsive to global challenges, and oriented towards protecting the constitutional rights of citizens in cyberspace. The background above is interesting to be studied in a discussion along with two problems that will be studied and researched, namely:

1. How are the current legal regulations on cyber security in facing the challenges of globalization?
2. How to improve the effectiveness of legal regulations on cybersecurity in the era of globalization to protect human rights and privacy?

2. METHODS

This study uses a normative legal research method, namely research that aims to examine the applicable positive legal norms related to cybersecurity regulations in the era of globalization. Normative legal research focuses on the study of relevant laws and legal principles, and aims to find the suitability, strengths, and weaknesses of legal norms in responding to the dynamics of cross-border cyber threats. This study uses several approaches, including a legislative approach to examine regulations in force in Indonesia such as Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE), Law Number 27 of 2022 concerning Personal Data Protection, and other regulations that support national

in the field that are cross-border and transnational. Global challenges in the field of cybersecurity include issues of harmonization of regulations between countries, limited jurisdiction of law

Journal of Sustainable Development Science
Vol. 7, No. 2, December 2025, pp. 99-106
e-ISSN: 2715-9140 **|** p-ISSN: 2722-919X

cybersecurity governance. In addition, a conceptual approach is used to understand the definition, characteristics, and legal principles underlying cybersecurity issues and human rights protection in the digital realm. The data used in this study are secondary data obtained through literature studies, which include primary legal materials in the form of laws and regulations, secondary legal materials such as academic literature, law journals, and expert opinions, and tertiary legal materials such as legal dictionaries and encyclopedias. The analysis technique used is qualitative analysis, which is carried out by interpreting and reviewing the contents of legal norms in depth to then be compiled in a descriptive-analytical form in order to answer the formulation of the problems that have been set. (Hosnah et al., 2021)

3. RESULT AND DISCUSSION

3.1 *Current Legal Regulations on Cyber Security in Facing the Challenges of Globalization.*

Facing the challenges of globalization marked by the rapid growth of information and communication technology, cybersecurity has become a strategic issue that cannot be ignored by any country, including Indonesia. Cyberspace has become a new arena in global interactions that recognize no geographical boundaries. However, behind the ease of access and exchange of information, globalization also brings consequences in the form of increasing risks of cybercrime and attacks that are cross-border and have a broad impact on national security, economy, politics, and the protection of human rights in cyberspace. (Kristanto & Baihaki, 2023)

Legal regulations regarding cybersecurity in Indonesia are currently fragmentary and spread across various laws and regulations. The most basic legal instrument is Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE) and its amendments. This law regulates various forms of violations and crimes that occur in the digital space, including illegal access, the spread of false information, and electronic insults or defamation. However, the ITE Law does not comprehensively regulate the national cyber defense strategy, the protection of vital information infrastructure, and the state's response to systemic and organized cyber attacks.

In addition to the ITE Law, Indonesia has also passed Law Number 27 of 2022 concerning

Personal Data Protection Act (PDP Act), which is an important advancement in protecting individual privacy rights in the digital era. This Act provides a legal basis for the management of personal data by both public and private parties, and regulates sanctions for violations of these rights. Personal data protection is one of the important pillars of cybersecurity, because it is directly related to efforts to prevent information leaks that can be used for further cyber attacks.

On the institutional side, Indonesia has the National Cyber and Crypto Agency (BSSN) as the main institution responsible for formulating policies and implementing technical functions of national cybersecurity. BSSN has the authority to coordinate the protection of national information systems, mitigate cyber incidents, and develop cyber defense capacity. Although the role of BSSN is quite central, cross-sector coordination and

Journal of Sustainable Development Science
Vol. 7, No. 2, December 2025, pp. 99-106
e-ISSN: 2715-9140 **|** p-ISSN: 2722-919X

clarity of authority boundaries between agencies are still challenges in practice.

The biggest challenge of Indonesia's cybersecurity legal regulation is the transnational nature of the threat, so it cannot be resolved solely through national legal instruments. Cyber attacks can originate from actors outside the country's jurisdiction, complicating the investigation and law enforcement process. (Hermawanto & Anggraini, 2020) In addition, the absence of a specific law that comprehensively regulates national cyber security and resilience is a significant legal vacuum. The draft Cyber Security and Resilience Law (RUU KKS) that is currently being drafted is expected to be a solution to this vacuum, but until now the discussion has not been completed and still raises controversy in society, especially regarding the potential for violations of civil liberties and democratic digital space. In a global context, national legal regulations are also not fully in harmony with international norms such as the Budapest Convention on Cybercrime, which is the global standard for combating cybercrime. (Schmitt, 2013) Indonesia is not yet a party to this convention, so the space for international cooperation in terms of extradition, mutual legal assistance, and exchange of information is still limited. (Kristianti & Kurniasi, 2024)

Thus, it can be concluded that the legal regulation on cybersecurity in Indonesia currently has an important initial foundation, but still faces various conceptual and structural obstacles in responding to the complexity of global threats. Therefore, strategic steps are needed in the formation of more holistic regulations, strengthening institutions, increasing human resource capacity, and expanding international cooperation in order to build a strong, resilient, and adaptive national cybersecurity system to the development of the times.

3.2 *Effectiveness of Legal Regulations on Cyber Security in the Era of Globalization to Protect Human Rights and Privacy.*

The era of digital globalization marked by advances in information and communication technology, legal regulations regarding cybersecurity are not only intended to protect digital infrastructure from attacks or disruptions, but must also be able to guarantee protection of human rights (HAM), especially the right to privacy, freedom of expression, and freedom of access to information. Digital space is an extension of conventional public space which is increasingly important in social, economic, political activities, and even in implementing democracy. Therefore, the biggest challenge in increasing the effectiveness of current cybersecurity legal regulations is not only in the technical aspects of defense, but also in how the state is able to balance security interests and the protection of citizens' civil rights.

Along with the increasing intensity of the use of digital technology, various violations of individual privacy rights often occur. Cases of personal data leaks, digital surveillance without a strong legal basis, and misuse of information by certain parties show that existing legal regulations are still weak in guaranteeing people's privacy rights. In this context, the presence of Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) is an important milestone that provides a legal basis for individual control over their personal data. This law requires data controllers and processors to comply with

Journal of Sustainable Development Science
Vol. 7, No. 2, December 2025, pp. 99-106
e-ISSN: 2715-9140 | p-ISSN: 2722-919X

data protection principles, such as the principles of transparency, purpose limitation, and processing security.

However, the effectiveness of the PDP Law still depends heavily on its technical and institutional implementation. The absence of an independent supervisory authority that specifically oversees the implementation of the PDP Law, as well as the low digital literacy of the community in understanding their rights, are serious challenges in enforcing real protection of privacy rights. In addition, the administrative and criminal sanctions stipulated in the law have not fully created a deterrent effect, especially against large-scale violations involving global technology companies.

From the cybersecurity side, human rights protection efforts must also be reflected in the policy mechanisms and technical regulations issued by the government, especially by the National Cyber and Crypto Agency (BSSN). Any form of supervision, tracking, or blocking of content in the digital space must be implemented proportionally, accountably, and in accordance with the principle of due process of law. (Anwar & Sanmorino, 2024) Administrative decisions to restrict access to information or collect data must not be made arbitrarily, but must be based on legitimate interests, such as maintaining national security or public order, and must be subject to transparent and legally testable procedures.

To improve the effectiveness of legal regulations in protecting human rights in cyberspace, there are several strategic steps that can be taken. First, it is necessary to draft a special law on cybersecurity that contains strict regulations but still guarantees democratic principles and the protection of individual rights. This law must regulate the limits of state authority in carrying out digital intervention, law-based supervision, and guarantees of data protection and personal communications. (Rusydi, 2025)

Second, institutional strengthening and coordination between agencies are needed, including between BSSN, Komnas HAM, Kominfo, and law enforcement officers, so that cybersecurity regulations do not overlap and continue to uphold the principle of checks and balances in their implementation. Third, increasing the capacity of human resources and technological infrastructure is very important, especially among law enforcement officers and electronic system organizers, so that they are able to understand the principles of human rights protection in a digital context.

Fourth, there must be increased international cooperation that allows for the exchange of information, harmonization of data protection standards, and collaboration in dealing with cross-border cyber violations. Many international norms can be used as references, such as the International Covenant on Civil and Political Rights (ICCPR), the General Data Protection Regulation (GDPR) of the European Union, and the Budapest Convention on Cybercrime as standards for transnational law enforcement cooperation.

Thus, the effectiveness of cybersecurity legal regulations in protecting human rights and privacy lies not only in the existence of legal norms, but also in consistent implementation, independent supervision, and a strong understanding of human rights principles amidst the challenges of technology and globalization. The state must be able to build a digital space governance that is safe, inclusive,

Journal of Sustainable Development Science
Vol. 7, No. 2, December 2025, pp. 99-106
e-ISSN: 2715-9140 **|** p-ISSN: 2722-919X

and continues to uphold the dignity and freedom of individuals as fundamental elements in a democratic state of law.

4. CONCLUSIONS

The legal regulation on cybersecurity in Indonesia currently has a normative basis through several legal instruments, such as the Electronic Information and Transactions Law (UU ITE), the Personal Data Protection Law (UU PDP), and the establishment of the National Cyber and Crypto Agency (BSSN). However, these regulations are still partial, sectoral, and have not been fully able to answer the challenges of globalization that present cross-border cyber threats. The absence of a specific law that comprehensively regulates national cybersecurity and resilience is one of the main weaknesses in facing the dynamics of global threats in the digital space.

The effectiveness of cybersecurity legal regulations in protecting human rights and privacy still faces various challenges, both normatively, institutionally, and in implementation. Although the presence of the PDP Law is a step forward in protecting personal data, its implementation has not been optimal due to the lack of an independent supervisory authority and the low digital literacy of the community. In addition, efforts to secure cyberspace by the state are often not balanced with the protection of civil rights such as privacy, freedom of expression, and access to information. Therefore, it is necessary to update the law that not only strengthens the national security system, but also emphasizes the principles of democracy and human rights in managing digital space.

ACKNOWLEDGMENT

The author would like to express his deepest gratitude to all parties who have provided support, both directly and indirectly, in completing this research. Thank you to those who have provided very meaningful guidance and direction during this research process. Thank's are also expressed to those who have provided facilities and resources which were very helpful in preparing this research.

REFERENCE

Anwar, Y. Z., & Sanmorino, A. (2024). Hukum dan Kebijakan Keamanan Siber: Tantangan Regulasi Perangkat IoT. *Jurnal Ilmiah Informatika Global*, *15*(3), 95–99. https://doi.org/DOI: https://doi.org/10.36982/jiig.v15i3.4773

Budhijanto, D. (2024). *Hukum keamanan siber: Teori, regulasi, dan implementasi dalam masyarakat digital*. Logoz Publishing.

Hermawanto, & Anggraini, M. (2020). Globalization, digital revolution, and locality. *LPPM Press*, 53.

Hosnah, A., Wijanarko, D., & Sibuea, H. (2021). *Characteristics of legal science and normative legal research methods*. RajaGrafindo Persada.

Jennings-Trace, E. (2025). *AI powering a "dramatic surge" in cyberthreats as automated scans hit 36,000 per second*. TechRadarTechRadar the Business Technology Experts. https://www.techradar.com/pro/security/ai-powering-a-dramatic-surge-in-cyberthreats-as-automated-scans-hit-36-000-per-second

Judijanto, L., & Nugroho, B. (2025). Regulasi Keamanan Siber dan Penegakan Hukum terhadap Cybercrime di Indonesia. *Sanskara Hukum Dan HAM (SHH)*, *3*(3), 118–124. https://doi.org/https://doi.org/10.58812/shh.v3i03.544

Klepper, D. (2025). *US imposes sanctions on Russian and Iranian groups over disinformation targeting American voters*. Apnews.Com.

Journal of Sustainable Development Science
Vol. 7, No. 2, December 2025, pp. 99-106
e-ISSN: 2715-9140 **|** p-ISSN: 2722-919X

https://apnews.com/article/russia-iran-trump-disinformation-election-959d3f36ffc81f3e5d07386122076e7e

Kristanto, K., & Baihaki, R. (2023). *Cybercrime in Indonesia: Regulation, challenges, and law enforcement*. Media Penerbit Indonesia.

Kristianti, N., & Kurniasi, R. (2024). Cybersecurity rules and regulations in the digital era. *Satya Dharma Journal of Law*, *7*(1), 44–59.

Novita, D., Utami, W., & Hartati, R. (2024). The development of cyber law in Indonesia: A literature study in the context of globalization. *Innovative: Journal of Social Science Research*, *4*(6), 100–115.

Reuters. (2024). *Ukraine's Kyivstar allocated $90 million to deal with cyberattack aftermath*. Reuters. https://www.reuters.com/technology/cybersecurity/ukraines-kyivstar-allocated-90-million-deal-with-cyberattack-aftermath-2024-05-20/

Rusydi, M. (2025). Comparison of Indonesian cyber law with ASEAN countries: A normative study. *Collaborative Journal of Science*, *8*(1), 15–28.

Schmitt, M. N. (Ed.). (2013). Tallinn manual on the international law applicable to cyber warfare. *Cambridge: Cambridge University Press.*

Sodiq, M., Rachman, R., & Wulandari, F. (2024). Cyber espionage policy and regulation in Indonesia: A comparative study of Indonesia–Germany. *Journal of Education, Social, and Culture*, *10*(1), 55–69.

Tobing, C., Wahyuni, A., & Rahmawati, D. (2024). Digital globalization and cybercrime: Legal challenges in the era of open information. *Sasana Law Journal*, *10*(2), 122–135.