Sustainable Development in the Digital Era: The Role of Cyber Law in Ensuring Security, Justice, and Legal Certainty

Novembryan Prayitno Putra[1], Hani Irhamdessetya[2]
[1,2] Universitas Ngudi Waluyo
Email Correspondence: novembryanprayitno@gmail.com

Abstract

The rapid development of digital technology has fundamentally transformed various sectors of social life, including the economy, governance, and law enforcement. While digitalization offers significant opportunities to accelerate development and enhance efficiency, it also generates new legal risks such as cybercrime, threats to electronic system security, violations of personal data protection, and potential infringements of human rights. In the framework of the 2030 Agenda for Sustainable Development, particularly Sustainable Development Goal (SDG) 9 on resilient infrastructure and innovation and SDG 16 on justice and strong institutions, cyber law plays a strategic role in ensuring that digital transformation proceeds in a secure, just, and legally certain manner. This study employs a normative legal research method using statutory and conceptual approaches to analyze Indonesia's cyber law framework, primarily the Law on Electronic Information and Transactions (ITE Law) and the Law on Personal Data Protection (PDP Law). The analysis demonstrates that cyber law contributes to sustainable development through three core functions. First, it ensures cybersecurity by protecting electronic systems and data from cyber threats, thereby supporting resilient digital infrastructure and economic stability. Second, it promotes justice and human rights protection by safeguarding privacy rights and positioning individuals as legal subjects in the digital sphere. Third, it provides legal certainty by recognizing electronic transactions and electronic evidence as legally valid, thus fostering public trust and sustainable digital economic growth. Despite its strategic role, the implementation of cyber law faces challenges, including regulatory disharmony, limited law enforcement capacity, and the rapid pace of technological change. This study concludes that cyber law must be continuously reformed and harmonized to effectively support sustainable development, ensuring that digital transformation aligns with the principles of security, justice, and legal certainty in accordance with SDG 9 and SDG 16.

Keywords: Cyber Law; Sustainable Development; Cybersecurity, Legal Certain;, Human Rights, SDGs.

Introduction

The development of digital technology has brought fundamental structural changes to almost all aspects of social life, including the economic, social, political, governmental, and law enforcement sectors. Digitalization has driven the emergence of electronic transactions, platform-based digital economies, digital financial services, and the implementation of electronic government (e-government).(Szerb et al., 2022) On the one hand, this digital transformation opens significant opportunities for accelerating national development, improving the efficiency of public services, and strengthening economic competitiveness. On the other hand, however, rapid technological advancement has also generated new legal risks(Kavanagh, 2022), such as cybercrime, threats to electronic system security, violations of personal data protection, and potential infringements of human rights in the digital sphere.

In the global context, sustainable development as formulated in the 2030 Agenda for Sustainable Development Goals (SDGs) positions technology and innovation as essential instruments of development while emphasizing the importance of fair and law-based governance.(Trubek & Trubek, 2006) Specifically, SDG 9 emphasizes the development of resilient infrastructure, inclusive industrialization, and sustainable innovation, whereas SDG 16 focuses on strengthening effective and accountable institutions, law enforcement, and the protection of human rights. In the digital era, the achievement of these two goals is highly dependent on the existence and effectiveness of cyber law.

The legal regulation of the digital sphere in Indonesia was normatively initiated through Law Number 11 of 2008 on Electronic Information and Transactions, as amended by Law Number 19 of 2016 (the ITE Law).(Siregar et al., 2020) From the perspective of legal certainty, the ITE Law

provides a legal foundation for digital activities through Article 1 point 2, which recognizes electronic transactions as legally valid acts. Furthermore, Article 5 paragraphs (1) and (2) affirm that electronic information and/or electronic documents constitute valid legal evidence, thereby ensuring legal certainty for transactions and legal activities conducted in the digital environment. These provisions directly contribute to the achievement of SDG 9, as legal certainty is a fundamental prerequisite for digital economic growth and technological innovation.

Similarly, the enactment of the Personal Data Protection Law (Law Number 27 of 2022) as a new legal regime has prompted numerous normative studies on privacy rights and the obligations of data controllers. However, research that examines the Personal Data Protection Law integratively as an instrument of sustainable development and institutional strengthening, as mandated by SDG 16, remains limited. Most existing studies have not explicitly linked the principles of personal data processing under Article 20 of the PDP Law with the concepts of justice, accountability, and legal certainty in long-term digital governance.

In addition, there exists a gap between the development of cyber law regulations and their implementation in law enforcement practice. Academic studies that critically map the tensions between legal certainty, cybersecurity, and the protection of human rights in the application of the ITE Law and the PDP Law remain relatively scarce. This tension, however, constitutes a central issue in ensuring that digital transformation not only promotes economic growth but also strengthens social justice and effective legal institutions.

Based on these conditions, the research gap in this study lies in the absence of a comprehensive and integrative legal analysis of cyber law particularly the ITE Law and the Personal Data Protection Law from the perspective of sustainable development, with a specific focus on ensuring security, justice, and legal certainty as prerequisites for achieving SDG 9 and SDG 16. This study seeks to fill this gap by offering a normative conceptual approach that connects cyber law, sustainable development, and equitable digital governance.

Accordingly, the urgency of this research lies not only in the academic need to enrich the discourse on cyber law, but also in the practical necessity of providing an analytical framework for policymakers and law enforcement authorities in formulating and implementing cyber law that is adaptive, just, and oriented toward sustainable development in the digital era.

From a security perspective, the ITE Law contains provisions aimed at protecting electronic systems and users from various cyber threats. Article 30 regulates the prohibition of unauthorized access to electronic systems, while Articles 31 and 32 prohibit interception as well as the alteration(Reese, 2003), deletion, or destruction of electronic information. The criminal provisions set forth in Articles 46 to 48 further reinforce the protection of electronic system security. These regulations demonstrate the role of cyber law in creating a secure digital environment as the foundation for sustainable digital infrastructure development, in line with the objectives of SDG 9.

Nevertheless, from the perspective of justice and human rights protection, the implementation of the ITE Law continues to face significant challenges. Provisions concerning prohibited acts under Article 27 paragraphs (1) to (4) as well as Articles 28 and 29 of the ITE Law have frequently generated debate regarding the limits of freedom of expression and the potential criminalization of citizens. This situation illustrates that sustainable digital development cannot rely solely on security and economic growth, but must also ensure legal justice and the protection of digital rights, as emphasized in SDG 16.

Awareness of the importance of privacy protection in the digital era subsequently led to the enactment of the Personal Data Protection Law (Law Number 27 of 2022). From a justice perspective, Article 4 of the PDP Law affirms that personal data constitute part of the inherent rights of data subjects, thereby imposing an obligation on the state to ensure their protection. This recognition strengthens the human rights dimension of the digital sphere and directly supports the achievement of SDG 16, particularly with regard to rights protection and access to justice.

From the perspective of legal certainty and governance, Article 20 of the PDP Law sets forth fundamental principles for personal data processing, including legality, purpose limitation, transparency, and accountability. These provisions provide clear normative guidance for data controllers and processors in conducting digital activities responsibly. Furthermore, regulations concerning the obligations of data controllers under Articles 35 and 36, as well as administrative and criminal sanctions under Articles 57 to 67 of the PDP Law, demonstrate the state's commitment to ensuring data security and building public trust in the digital ecosystem. Such trust is a key element in sustaining innovation and digital economic development, as envisaged under SDG 9.

Thus, cyber law in Indonesia reflected in the ITE Law and the Personal Data Protection Law(Purtova, 2018) plays a strategic role in ensuring digital security, legal justice, and legal certainty as the foundation of sustainable development in the digital era. Nevertheless, implementation challenges remain significant, including regulatory disharmony, limitations in law enforcement capacity, and regulatory lag behind rapid technological advancements.(Marchant, 2011) These conditions underscore the necessity of a comprehensive and critical study on the role of cyber law in supporting the achievement of SDG 9 and SDG 16, while ensuring that digital transformation proceeds in accordance with the principles of sustainable development.

Accordingly, the study entitled "Sustainable Development in the Digital Era: The Role of Cyber Law in Ensuring Security, Justice, and Legal Certainty" is both theoretically and practically significant. From a theoretical standpoint, this research contributes to the development of cyber law concepts oriented toward sustainability and human rights. From a practical standpoint, it is expected to serve as a reference for policymakers and law enforcement authorities in formulating and implementing cyber law capable of addressing the challenges of digital transformation while supporting the sustainable achievement of SDG 9 and SDG 16. Based on the foregoing background, the research problems in this study are formulated as follows: What is the role of cyber law in supporting sustainable development in the digital era? And How does cyber law function in ensuring security, justice, and legal certainty in cyberspace?

Method of Analysis (Legal Research Method)

This study employs a normative legal research method, which conceptualizes law as a set of norms or rules governing conduct within the positive legal system. This method is selected because the research focuses on analyzing the role of cyber law in supporting sustainable development and in ensuring security, justice, and legal certainty in the digital era.

The approaches applied in this study include the statutory approach and the conceptual approach. The statutory approach is used to examine and analyze regulations related to cyber law, particularly the Law on Electronic Information and Transactions (ITE Law) and the Law on Personal Data Protection (PDP Law).(Simbolon & Juwono, 2022) Meanwhile, the conceptual approach is employed to examine the concepts of sustainable development, legal justice, legal certainty, and the protection of human rights in the digital sphere.

The legal materials used in this study consist of primary legal materials, namely statutory regulations relevant to cyber law, and secondary legal materials, including legal textbooks, scholarly journals, and national as well as international policy documents related to sustainable development and digital governance. The collection of legal materials is conducted through library research.

The analysis of legal materials is carried out using a qualitative normative method, by systematically interpreting legal norms and linking them to theories and principles of sustainable development,(Barral, 2012) particularly those related to Sustainable Development Goal (SDG) 9 and Sustainable Development Goal (SDG) 16. The results of this analysis are then used to draw conclusions regarding the role and function of cyber law in ensuring security, justice, and legal certainty as the foundation of sustainable development in the digital era.

Result and Discussion

Result

Cyber Law as a Pillar of Security in Sustainable Development

Security constitutes a fundamental element of sustainable development in the digital era. Cyber law plays a crucial role in establishing a legal protection framework against cyber threats(Chander & Kaur, 2022), including hacking, data theft, and other forms of cybercrime. Through the existence of clear and comprehensive regulations on cybersecurity, the State is able to protect strategic digital infrastructure and maintain public as well as business trust in the digital ecosystem.

Discussion

The Role of Cyber Law in Supporting Sustainable Development in the Digital Era (with Legal Basis)

The development of digital technology has transformed cyberspace into one of the primary infrastructures of national development. Within the framework of sustainable development, digital transformation is not merely perceived as a means of economic growth, but also as an instrument for achieving social justice, protecting human rights, and strengthening effective legal institutions.

Accordingly, cyber law plays a strategic role as a normative framework governing the use of digital technology in order to ensure its alignment with the principles of sustainable development and global development objectives.

First, from the perspective of legal certainty and digital economic growth, cyber law functions as a normative foundation for technology based economic activities(De Vries et al., 2012). The legal recognition of electronic transactions and electronic documents as valid legal acts provides legal certainty for business actors and society at large. In the Indonesian context, this legal basis is explicitly reflected in Article 1 point 2 of the Electronic Information and Transactions Law (ITE Law), which defines electronic transactions as legal acts conducted using computers, computer networks, and/or other electronic media. Furthermore, Article 5 paragraphs (1) and (2) of the ITE Law affirm that electronic information and/or electronic documents constitute valid legal evidence.

These provisions confer legal legitimacy upon digital economic activities, including e-commerce, digital financial services, and electronic contracts. Such legal certainty enhances public trust, stimulates investment in the digital economy sector, and fosters an enabling environment for sustainable technological innovation. In this respect, cyber law directly contributes to the achievement of Sustainable Development Goal (SDG) 9, which emphasizes the development of resilient infrastructure, inclusive industrialization, and sustainable innovation.

Second, from the perspective of security and the resilience of digital infrastructure, cyber law plays a crucial role in protecting electronic systems and data from various cyber threats. Digital security constitutes a fundamental prerequisite for sustainable development in the digital era, as failures in ensuring cybersecurity may result in systemic impacts on economic stability, public services, and public trust. The ITE Law normatively provides such protection through several provisions, including Article 30, which prohibits unauthorized access to electronic systems; Article 31, which regulates the prohibition of unlawful interception; and Article 32, which prohibits the unlawful alteration, destruction, or transfer of electronic information.

The criminal sanctions stipulated in Articles 46 to 48 of the ITE Law further reinforce this protective function by imposing penalties for violations of electronic system security(Siponen & Vance, 2010). These regulatory measures demonstrate that cyber law serves not only a repressive function but also a preventive one in safeguarding the sustainability of the digital ecosystem. By establishing a secure and reliable digital environment, cyber law supports the development of sustainable digital infrastructure in line with the objectives of SDG 9.

Third, from the perspective of social justice and the protection of human rights, cyber law plays a pivotal role in ensuring that digital transformation does not generate new forms of injustice.(Mihr, 2017) An inadequately regulated digital space may lead to violations of privacy rights, misuse of personal data, and the marginalization of certain groups. Awareness of the importance of privacy protection has led to the enactment of Law Number 27 of 2022 on Personal Data Protection (PDP Law) as a specific legal regime governing personal data.

Normatively, Article 4 of the PDP Law affirms that personal data constitute part of the personal rights of data subjects, thereby imposing upon the State an obligation to ensure their protection. This provision strengthens the human rights dimension of the digital sphere and positions individuals as legal subjects who must be safeguarded from arbitrary data processing practices. The protection of digital rights constitutes an integral component of people-centered sustainable development, while simultaneously supporting the achievement of SDG 16, which emphasizes justice, human rights protection, and access to justice.

Fourth, from the perspective of governance and the strengthening of legal institutions, cyber law contributes to the development of a legal system that is adaptive to technological advancements. Sustainable development requires legal institutions capable of effectively responding to social and technological change. In this regard, cyber law provides the legal framework for the implementation of digital government (e-government), cyber law enforcement, and the accountability of electronic system operators. For instance, Articles 15 and 16 of the ITE Law regulate the obligations of electronic system operators to ensure that their systems are reliable, secure, and responsibly managed.

In addition, Article 20 of the PDP Law stipulates fundamental principles of personal data processing, including lawfulness, transparency, purpose limitation, and accountability. These principles reinforce good digital governance and enhance public trust in both state institutions and private sector actors. Through clear and structured regulatory frameworks, the State is better positioned to exercise oversight and law enforcement functions in cyberspace, thereby supporting the objectives of SDG 16 in building strong, effective, and accountable institutions.

Nevertheless, the strategic role of cyber law in supporting sustainable development is not without challenges(Ige et al., 2024). Rapid technological advancements often outpace regulatory reforms, creating potential gaps between legal norms and practical implementation. Moreover, regulatory disharmony, normative ambiguity, and limited law enforcement capacity continue to constrain the optimal functioning of cyber law. Accordingly, sustained legal reform, justice oriented legal interpretation, and the strengthening of institutional capacity are necessary to ensure that cyber law can effectively address the challenges of sustainable development in the digital era.

Thus, it can be concluded that cyber law plays a central role in supporting sustainable development through the creation of legal certainty (ITE Law), protection of cyber security (ITE Law), guaranteeing justice and human rights (PDP Law), and strengthening accountable legal governance and institutions (ITE Law and PDP Law). This role makes cyber law a strategic legal instrument that not only regulates the use of digital technology, but also ensures that digital transformation is in line with the principles of sustainable development and the objectives of SDG 9 and SDG 16.

The Role of Cyber Law in Ensuring Security, Justice, and Legal Certainty in Cyberspace

The existence of cyberspace as an integral component of social, economic, and governmental life necessitates a legal system capable of ensuring security, justice, and legal certainty. Cyber law serves as a normative instrument governing legal conduct in the digital environment while simultaneously addressing various risks arising from the utilization of information technology. In the Indonesian context, this function is primarily embodied in Law Number 11 of 2008 on Information and Electronic Transactions, as amended by Law Number 19 of 2016 (the ITE Law), and Law Number 27 of 2022 on Personal Data Protection (the PDP Law).

Ensuring Cybersecurity(Ige et al., 2024)

Cybersecurity constitutes a fundamental prerequisite for the sustainability of digital activities. In the absence of adequate security guarantees, cyberspace is highly vulnerable to misuse for cybercrimes such as hacking, data theft, online fraud, and sabotage of electronic systems. Cyber law functions as both a preventive and repressive legal instrument in addressing such threats.

Normatively, the ITE Law regulates prohibitions against various forms of violations of electronic system security. Article 30 of the ITE Law prohibits any person from unlawfully accessing computers and/or electronic systems belonging to others, whether for the purpose of obtaining information or breaching system security. Furthermore, Article 31 of the ITE Law prohibits unlawful interception or wiretapping of electronic information and/or electronic documents, while Article 32 prohibits the unlawful alteration, destruction, deletion, or transfer of electronic information.

These prohibitions are reinforced by criminal sanctions stipulated in Articles 46 to 48 of the ITE Law, which underscore the law enforcement function in safeguarding cybersecurity. The imposition of criminal sanctions serves not only a repressive function but also a preventive one, by providing a deterrent effect against potential cyber offenders.

In addition, the security aspect is further strengthened through the obligations imposed on electronic system operators. Articles 15 and 16 of the ITE Law require electronic system operators to ensure that their systems are reliable, secure, and responsibly managed. These provisions affirm that cybersecurity is not solely the responsibility of the state, but also of business actors and institutions that operate electronic systems.

Accordingly, cyber law functions as a normative pillar in ensuring cybersecurity, which in turn supports the stability of the digital economy, the protection of public services, and public trust in digital technologies.

Ensuring Justice in Cyberspace(First & Hart, 2002)

Beyond security considerations, cyber law also plays a crucial role in ensuring justice, particularly in relation to the protection of human rights and the equality of legal standing among parties in the digital sphere. Digital transformation has the potential to generate new forms of inequality if not accompanied by fair and rights-based regulation.

The PDP Law represents a significant milestone in ensuring digital justice, particularly with regard to the protection of privacy rights. Article 4 of the PDP Law affirms that personal data constitute part of the personal rights of data subjects, thereby obligating that all personal data

processing activities respect human dignity and fundamental human rights. Furthermore, Articles 5 to 13 of the PDP Law regulate the rights of data subjects, including the right to information, the right to access and rectify personal data, the right to withdraw consent, and the right to erasure of personal data.

These provisions reflect the principle of substantive justice, as they position individuals as active and protected legal subjects, rather than mere objects of data processing by the state or corporations. In this context, cyber law functions as a safeguard against abuses of power in the management of data and digital technologies.

In addition, the ITE Law contributes to the realization of justice through its regulation of legal responsibility and evidentiary mechanisms. The recognition of electronic information and/or electronic documents as lawful evidence, as stipulated in Article 5 paragraphs (1) and (2) of the ITE Law, provides equal opportunities for parties to seek justice in judicial proceedings, particularly in cases involving information technology.

Thus, cyber law serves as a legal instrument for realizing justice in cyberspace by ensuring the protection of digital rights, balancing competing interests, and guaranteeing access to justice for all citizens.

Ensuring Legal Certainty in Cyberspace

Legal certainty constitutes one of the fundamental objectives of law, especially within a digital society characterized by speed, complexity, and cross-border interactions. Without legal certainty, the utilization of digital technology may generate uncertainty in legal relationships, whether in economic transactions, communication, or public service delivery.

Cyber law provides legal certainty through the formulation of clear norms regarding the legal status of electronic acts and electronic evidence. Article 1 point 2 of the ITE Law defines electronic transactions as legal acts conducted using computers, computer networks, and/or other electronic media. This definition affirms that digital activities carry legal consequences equivalent to those of conventional legal acts.

Furthermore, Article 5 of the ITE Law, which recognizes electronic information and/or electronic documents as lawful evidence, provides clarity in law enforcement practices and dispute resolution mechanisms. This legal certainty is essential in supporting e-commerce activities, digital financial services, and electronic contracts, as parties are afforded legal guarantees concerning their rights and obligations.

In the realm of personal data protection, the PDP Law also ensures legal certainty through the regulation of personal data processing principles, as stipulated in Article 20, including lawfulness, transparency, purpose limitation, and accountability. These principles serve as clear guidelines for data controllers and data processors in fulfilling their legal obligations.

Through the establishment of a clear legal framework, cyber law functions to reduce legal uncertainty, prevent multiple interpretations of legal norms, and enhance consistency in law enforcement within cyberspace.

Relevance to Sustainable Development

The function of cyber law in ensuring security, justice, and legal certainty is closely linked to the objectives of sustainable development. Cybersecurity supports the development of resilient digital infrastructure (SDG 9), while justice and legal certainty contribute to the strengthening of effective institutions, the protection of human rights, and access to justice (SDG 16).

Nevertheless, the effectiveness of cyber law continues to face challenges, including the rapid pace of technological advancement relative to regulatory reform, regulatory disharmony, and limitations in law enforcement capacity. Therefore, continuous legal reform, regulatory harmonization, and institutional capacity building are required to ensure that cyber law can optimally fulfill its role in addressing the demands of sustainable development in the digital era.

Conclusion

Cyber law plays a highly strategic role in supporting sustainable development in the digital era, particularly through its core functions in ensuring security, justice, and legal certainty in cyberspace. The existence of cyber law can no longer be understood merely as an instrument for controlling technology-based crimes, but rather as a normative framework that directs the utilization of digital technology in line with national and global development objectives.

In the context of sustainable development, cyber law functions as a legal foundation for inclusive and sustainable digital economic growth by providing legal certainty for electronic transactions, protection of electronic systems, and recognition of digital evidence. Such legal certainty fosters public trust, enhances investment, and strengthens technological innovation oriented toward sustainability, in accordance with Sustainable Development Goal (SDG) 9, which emphasizes resilient infrastructure, inclusive industrialization, and sustainable innovation.

Furthermore, cyber law plays a crucial role in ensuring justice and the protection of human rights in the digital sphere. Through the regulation of personal data protection and the recognition of individual digital rights, cyber law positions human beings as the central subjects of digital transformation. This approach reflects a people-centered sustainable development paradigm and contributes to the achievement of SDG 16, which emphasizes justice, human rights protection, and the strengthening of effective, accountable legal institutions.

Moreover, cyber law serves as an instrument for strengthening governance and legal institutions in the digital era. Regulations governing the obligations of electronic system operators, principles of accountability, and cyber law enforcement mechanisms demonstrate that cyber law plays an important role in building a legal system that is adaptive to technological developments. Thus, cyber law not only regulates legal conduct in cyberspace but also directly contributes to social, economic, and governmental stability as key pillars of sustainable development.

In the Indonesian context, strengthening cyber law constitutes an urgent necessity in light of the rapid digital transformation across various sectors of life. Challenges arising from the rapid pace of technological development, the increasing complexity of cybercrime, and the potential for violations of digital rights demand a cyber legal framework that is comprehensive, adaptive, and grounded in justice. Therefore, cyber law must be positioned as a strategic instrument of the state to ensure that digital transformation proceeds in accordance with the principles of security, justice, legal certainty, and sustainable development.

Recommendations

Based on the foregoing conclusions, several recommendations may be proposed for the future development and strengthening of cyber law. First, efforts toward harmonizing cyber law regulations are necessary to ensure coherence among various statutory instruments governing digital technology, including the ITE Law, the Personal Data Protection Law, and other sectoral regulations. Such harmonization is essential to prevent normative overlap, multiple interpretations, and legal uncertainty in the enforcement of cyber law.

Second, enhancing the capacity and professionalism of law enforcement officials is of paramount importance. Effective enforcement of cyber law requires adequate understanding of information technology, digital forensic techniques, and the evolving dynamics of cybercrime. Accordingly, continuous training, strengthening of infrastructure, and cross sectoral as well as cross border cooperation must be consistently improved.

Third, strengthening the protection of citizens' digital rights should become a top priority in the development of cyber law. The state must ensure that cyber legal regulations are not solely oriented toward security and economic interests, but also guarantee the protection of privacy rights, responsible freedom of expression, and equitable access to digital technology. A human rights-based approach should be consistently integrated into the formulation and implementation of cyber law policies.

Fourth, the sustainable development approach should serve as a normative foundation in the formulation of cyber law policies. This includes integrating principles of sustainability, inclusivity, and intergenerational justice into cyber legal regulations, so that digital transformation not only provides short-term benefits but also ensures long-term social, economic, and legal sustainability.

Accordingly, the development of a comprehensive, adaptive, and sustainability-oriented cyber law framework is expected to effectively address the challenges of the digital era while positioning cyberspace as a secure, just, and constructive domain for societal and national advancement.

Acknowledgements

The author expresses sincere gratitude to all parties who have provided support and contributions in the preparation of this article. In particular, the author extends appreciation to the academic supervisor, Dr. Hani Irhamdessetya, S.H., M.H., as well as to the Faculty of Economics,

Law, and Humanities and the academic community of Universitas Ngudi Waluyo, for their academic support and the facilities provided, which enabled the completion of this research.

The author also wishes to thank colleagues for their valuable input, scholarly discussions, and critical insights that significantly contributed to the refinement of this article. Furthermore, sincere appreciation is extended to the editors and reviewers for their constructive suggestions and comments, which have enhanced the substance and quality of the writing. It is hoped that the findings of this research will contribute meaningfully to the development of legal scholarship, particularly in the fields of cyber law and sustainable development

References

Barral, V. (2012). Sustainable development in international law: nature and operation of an evolutive legal norm. *European Journal of International Law*, *23*(2), 377–400.

Chander, H., & Kaur, G. (2022). *Cyber laws and IT protection*. PHI Learning Pvt. Ltd.

De Vries, M. J., Hansson, S. O., & Meijers, A. W. M. (2012). *Norms in technology* (Vol. 9). Springer Science & Business Media.

First, P. F., & Hart, Y. Y. (2002). Access to cyberspace: The new issue in educational justice. *JL & Educ.*, *31*, 385.

Ige, A. B., Kupa, E., & Ilori, O. (2024). Aligning sustainable development goals with cybersecurity strategies: Ensuring a secure and sustainable future. *GSC Adv. Res. Rev*, *19*(3), 344–360.

Kavanagh, C. (2022). *New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?*. Carnegie Endowment for International Peace.

Marchant, G. E. (2011). The growing gap between emerging technologies and the law. *The Growing Gap between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem*, 19–33.

Mihr, A. (2017). *Cyber justice: Human rights and good governance for the internet*. Springer.

Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40–81.

Reese, R. A. (2003). Will merging access controls and rights controls undermine the structure of anticircumvention law? *Berkeley Tech. LJ*, *18*, 619.

Simbolon, V. A., & Juwono, V. (2022). Comparative review of personal data protection policy in Indonesia and the European Union General Data Protection Regulation. *Publik (Jurnal Ilmu Administrasi)*, *11*(2), 178–190.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 487–502.

Siregar, G., Siregar, S. A., & Silaban, R. (2020). Legal implementation of electronic information and transaction law in preventing the spread of content containing SARA issues through social media. *International Journal of Innovation Crativity and Change*, *13*(10), 1418–1431.

Szerb, L., Komlosi, E. S., Acs, Z. J., Lafuente, E., & Song, A. K. (2022). *The digital platform economy index 2020*. Springer.

Trubek, D. M., & Trubek, L. G. (2006). New governance & legal regulation: Complementarity, rivalry, and transformation. *Colum. J. Eur. L.*, *13*, 539.