DIPONEGORO
Law Review

Vol. 10, No. 1, April 2025 E-ISSN: 2527-4031
Available online at website: https://ejournal.undip.ac.id/index.php/dlr

ENHANCING CYBERSECURITY AND LEGAL INTEGRATION: REFORMING INDONESIA'S CYBER LAW TO FOSTER SUSTAINABLE GROWTH IN THE DIGITAL ECONOMY

Tri Fenny Widayanti, *Aditya Dwi Rohman, A. Nuril Zamharir Haris, Eka Merdekawati Djafar, Muhammad Zulfan Hakim

Faculty of Law, Universitas Hasanuddin, Makassar, Indonesia
***Corresponding author**: adityadwirohman007@gmail.com

Abstract

The rapid advancement of digital technologies has reshaped the global economy, with the digital economy becoming a key driver of growth and innovation. Indonesia, as the leader in Southeast Asia's digital economy, has immense potential, with projected growth at 40% by 2018. However, the country's digital economy remains hindered by an inadequate and fragmented cyber law framework. The existing laws are sector-specific, leading to overlapping institutional authority, weak enforcement, and a lack of clarity in jurisdiction, particularly regarding cross-border cyber threats. This fragmented legal landscape impedes the integration of Indonesia's digital economy and undermines cybersecurity efforts. This study examines the challenges within Indonesia's current cyber law and argues for comprehensive reforms to provide clear institutional authority, enhance inter-agency coordination, and create laws tailored to the digital economy and cybersecurity. Drawing insights from international frameworks, such as the European Union's General Data Protection Regulation (GDPR) and Australia's Critical Infrastructure Bill, the study advocates for a dual approach—ensuring both data privacy and critical infrastructure protection. Furthermore, the research highlights the need for collaboration between government, the private sector, and civil society, along with public education initiatives, to foster a secure and trustworthy digital ecosystem. By analyzing existing regulations and proposing targeted reforms, this study aims to contribute to improved cybersecurity governance, enabling sustainable digital transformation and economic growth in Indonesia.

Keywords: *Cyber Law; Digital Economy; Cybersecurity; Regulatory Reform; Legal Development.*

Received: 19 January 2025; Revised: 25 April 2025; Accepted: 26 April 2025; Available online: 30 April 2025; Published: 30 April 2025.

How to Cite: Widayanti, Tri Fenny, Aditya Dwi Rohman, A. Nuril Zamharir Haris, Eka Merdekawati Djafar, and Muhammad Zulfan Hakim. "Enhancing Cybersecurity and Legal Integration: Reforming Indonesia's Cyber Law to Foster Sustainable Growth in the Digital Economy." *Diponegoro Law Review* 10, no. 1 (2025): 105–19. https://doi.org/10.14710/dilrev.10.1.2025.105-119.

1. Introduction

The rapid growth of digital technologies has fundamentally shaped the global economic landscape, resulting in the emergence of the digital economy as a key driver of growth, innovation, and development. Indonesia is the country in Southeast Asia with the largest digital economy and also the fastest growing with an estimated development rate of 40% in 2018.[1] As the largest country in Southeast Asia by population and with a swiftly expanding digital infrastructure, Indonesia holds a significant leadership position in the region's digital economy. However, despite these advances, Indonesia's legal framework for Cybersecurity and digital economy integration is widely considered ineffective and inefficient, failing to adequately address the complex challenges faced by cyber threats and digital transformation.

[1] Sinta Dewi Rosadi and Zahra Tahira, "Consumer Protection in Digital Economy Era: Law in Indonesia," *Yustisia* 7, no. 1 (2018). p. 85. https://doi.org/10.20961/yustisia.v7i1.20144

Indonesia's digital economy, despite growing rapidly, faces significant cybersecurity challenges. The increasing dependence on digital platforms and services makes businesses and individuals vulnerable to numerous cyber threats, such as data breaches, ransomware attacks, and online fraud. In addition, the lack of regulations specifically governing this issue [2] and comprehensive cybersecurity law enforcement mechanisms exacerbate these challenges, leaving organizations vulnerable to cyberattacks and undermining trust in digital transactions.

Indonesia, which controls 40% of the digital economy in ASEAN[3] and a total of more than 221 million internet users[4], has a very strong digital economy potential and will have a good impact on Indonesia's economic growth. However, the prevailing inadequacies and inefficiencies within Indonesia's cyber law framework hinder its ability to effectively address emerging cyber threats and promote a secure digital environment that supports economic growth and innovation. Despite cybersecurity-related laws and regulations, their enforcement and implementation remain inconsistent and tend to be sectoral[5] or fragmented, causing gaps in protection and enforcement. In this context, the development of a solid legal framework for Cybersecurity within the framework of digital economy integration is emerging as a critical imperative. Cyber Law covers a wide range of diverse legal issues relating to the use of the internet, including but not limited to privacy, data security, cyber crime, copyright, and other issues that arise in a digital context.[6] However, the current legal landscape in Indonesia is less effective in addressing the complex challenges faced by cyber threats and digital transformation, highlighting the urgent need for comprehensive reforms and policy interventions.

If Indonesia's cyber law issues are not properly addressed, significant social, economic, and legal consequences may arise. Socially, weak cybersecurity regulations can erode public trust in digital platforms, increase cybercrime victims, and exacerbate digital inequality.[7] Economically, inadequate legal frameworks hinder digital economy growth, deter foreign investment, and raise operational costs for businesses needing additional security measures.[8] Legally, fragmented regulations create uncertainty, weaken law enforcement against cybercrime, and limit international cooperation on cybersecurity. Together, these factors threaten Indonesia's economic potential, compromise online safety, and stifle innovation, emphasizing the urgent need for comprehensive legal reforms to support a secure and dynamic digital economy.

There are several paper that also explaining the same issue as what this paper will talk about, name it like Rumata[9] and Rosadi[10]. Unlike Rumata's research, which focuses primarily on the e-commerce sector as a key driver of digital growth, my research takes a broader approach by examining cyber law holistically within digital economy integration. Rumata identifies paradoxes in digital economy policies but does not directly tackle the legal harmonization needed

---

2 Sinta Dewi Rosadi and Garry Gumelar Pratama, "Urgensi Perlindungan Data Pribadi Dalam Era Ekonomi Digital Di Indonesia," *Veritas et Justitia* 4, no. 1 (2018). p. 90. https://doi.org/10.25123/vej.v4i1.2916

3 Kominfo Newsroom, "Indonesia Controls 40 Percent of ASEAN Digital Economy Market," ASEAN Indonesia 2023, August 14, 2023, asean2023.id/en/news/indonesia-controls-40-percent-of-asean-digital-economy-market.

4 APJII, "APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang," Asosiasi Penyelenggara Jasa Internet Indonesia, February 7, 2024, apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang.

5 Rosadi and Pratama, "Urgensi Perlindungan Data Pribadi Dalam Era Ekonomi Digital Di Indonesia."

6 Suryati et al., "Penguatan Literasi Digital Dalam Pencegahan Pelanggaran Hukum Siber (Cyber Law)," *Wajah Hukum* 8, no. 1 (2024): 84–94. http://dx.doi.org/10.33087/wjh.v8i1.1447

7 Bibi van den Berg and Esther Keymolen, "Regulating Security on the Internet: Control versus Trust," *International Review of Law, Computers & Technology* 31, no. 2 (May 4, 2017): 188–205, https://doi.org/10.1080/13600869.2017.1298504.

8 Carl Dahlman, Sam Mealy, and Martin Wermelinger, "Harnessing the Digital Economy for Developing Countries" (Paris, December 2016). p. 33. https://doi.org/10.1787/4adffb24-en

9 Vience Mutiara Rumata and Ashwin Sasongko Sastrosubroto, "The Paradox of Indonesian Digital Economy Development," in *E-Business - Higher Education and Intelligence Applications* (IntechOpen, 2021), https://doi.org/10.5772/intechopen.92140.

10 Rosadi and Pratama, "Urgensi Perlindungan Data Pribadi Dalam Era Ekonomi Digital Di Indonesia."

for comprehensive cybersecurity regulation. Meanwhile, Rosadi's study emphasizes the urgency of personal data protection, proposing privacy as a positive right with an international regulatory perspective. In contrast, my research extends beyond data protection to analyze gaps in cybersecurity governance, jurisdictional clarity, and cross-border enforcement issues. While Rosadi's work highlights specific aspects of data privacy, my study proposes an integrative legal framework to ensure sustainable cybersecurity governance and digital economic growth.

Together, all of those studies reveal the critical need for cohesive cyber law reform in Indonesia but differ in scope and focus, offering complementary perspectives on the nation's digital legal challenges. In this context, differ from other paper, this study aims to examine the development of cyber law in Indonesia within the framework of digital economy integration. By critically analyzing the existing legal landscape, identifying loopholes and shortcomings, and proposing implementable recommendations for reform, the study aims to contribute to improved cybersecurity governance, digital transformation, and sustainable development in Indonesia.

2. Method

This study adopts a normative juridical method, relying on both primary and secondary data sources, such as regulations, scholarly articles, and relevant references. [11] It uses a descriptive-analytical approach to explore the development of cyber law in Indonesia and its alignment with the growing integration of the digital economy. As the digital economy expands, so too does the need for effective cybersecurity governance, making it crucial to examine the adequacy of the existing legal frameworks. This research seeks to analyze how well current regulations match the rapidly evolving digital landscape, identifying any gaps, overlaps, or weaknesses in the law. A key part of this study is a qualitative analysis, which links normative legal principles with practical legal reasoning. By evaluating the effectiveness of current legislation, the research aims to provide actionable reform recommendations that could improve the country's cybersecurity measures. This includes suggesting updates to laws and regulations to ensure that they are in tune with technological advancements and digital economic trends. The data collection process is based on a comprehensive literature review and the evaluation of legislative documents, allowing for a thorough critique of regulatory issues. The findings of this study will not only shed light on the current state of cyber law in Indonesia but also offer legal strategies that can support a more sustainable digital transformation while reinforcing cybersecurity measures. This research ultimately aims to contribute to a stronger, more resilient digital infrastructure in Indonesia, helping the country navigate the complexities of the digital age with robust legal and regulatory frameworks.

3. Results and Discussion

3.1. Legal Landscape of Cybersecurity in Indonesia

There are several regulations in Indonesia that are directly related to cybersecurity that will support the digital economy in Indonesia. There are two regulations at the level of law, one government regulation, one presidential regulation, and one state institution regulation equivalent to the ministry. These regulations are, Law Number 27 of 2022 concerning Personal Data Protection or known as PDP Law, Law Number 11 of 2008 concerning Electronic Information and Transactions including its amendments in 2016 and 2024 known as the ITE Law, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, Government Regulation Number 80 of 2019 concerning Trading Through Electronic Systems, Presidential Regulation Number 47 of 2023 concerning National Cyber Security Strategy and Cyber Crisis Management, and BSSN Regulation Number 8 of 2020 concerning Security Systems in the Implementation of Electronic Systems.

Law No. 27 of 2022 on Personal Data Protection is a legislative measure addressing the critical need for a legal framework to manage personal data in the digital age. The PDP Law is designed to provide a legal framework for the protection of individuals' privacy rights and sets

[11] Soerjono Soekanto, *Pengantar Penelitian Hukum* (Jakarta: Universitas Indonesia, 1989).

standards for entities managing personal data, including obligations to maintain data confidentiality and security.[12] In the context of cybersecurity, the PDP Law is relevant as it addresses important aspects such as data leakage prevention, data breach notification, and cross-border data transfer, all of which are critical components in protecting data from cyberattacks. The sanctions established by the PDP Law aim to strengthen law enforcement and increase awareness and compliance with good data security practices.

The PDP Law outlines several key regulations to ensure the protection of personal data. It places significant responsibility on the data controller to maintain the confidentiality and security of personal data, requiring the implementation of both technical and organizational measures to safeguard it. In case of a data breach, the law mandates that the responsible party must notify the affected individual promptly, enabling them to take the necessary steps to protect themselves. Additionally, the law governs the transfer of personal data to other countries, ensuring that the destination country provides adequate data protection, often through written consent or security measures. Finally, the PDP Law stipulates sanctions for data violations, including fines and compensation for affected individuals, covering both financial and reputational damages.

Prior to the enactment of the PDP Law, Indonesia relied on Law No. 11 of 2008 regarding Electronic Information and Transactions, also known as the ITE Law, which plays a pivotal role in regulating various aspects of cybersecurity in the country. Among its key provisions, the ITE Law grants electronic signatures the same legal status as conventional signatures, ensuring their validity in legal transactions. The law also regulates the implementation of electronic certification and systems, facilitating secure and reliable digital transactions. It recognizes the legitimacy of electronic transactions in both public and private sectors, allowing parties involved to choose the applicable laws for international transactions. The ITE Law also governs domain names and intellectual property rights, protecting personal rights in these areas. It addresses cybercrimes in Chapter VII, Articles 27-37, and provides a mechanism for dispute resolution, allowing individuals to file lawsuits against electronic system operators or users causing harm. Additionally, the law mandates the government to protect public interest by regulating the misuse of electronic information and transactions that could disrupt public order. Finally, the investigation process under the ITE Law is carried out in accordance with the Criminal Procedure Code, with due regard for privacy protection, confidentiality, and the integrity of public services and data, ensuring compliance with legal frameworks.

Then there is Government Regulation Number 71 of 2019 which is an important regulation governing the Implementation of Electronic Systems and Transactions in Indonesia. This regulation replaces Government Regulation Number 82 of 2012 and is designed to provide legal certainty for business actors who operate electronic systems and transactions in their business activities. This GR specifically emphasizes the cybersecurity aspect by setting standards and procedures that must be followed by electronic system operators, both in the public and private spheres. This includes regulations on the use of electronic data, electronic transactions, and preventive and responsive measures against cybersecurity incidents.

At the GR level in addition to GR 71/2019, there is also Government Regulation of the Republic of Indonesia Number 80 of 2019 concerning Trading Through Electronic Systems which regulates various important aspects related to cybersecurity and personal data protection in electronic commerce. GR 80/2019 prioritizes the protection of personal data, which must be obtained honestly and legally, with security measures in place to prevent loss for data owners. Personal data should only be used for specific, legitimate purposes, and must be accurate and regularly updated, allowing data owners the opportunity to update their information. Additionally, the data-storing party must have adequate security systems to prevent data leakage or illegal use and be accountable for any unexpected losses. Transferring personal data abroad is permitted only if the destination country has a protection standard equivalent to Indonesia's. This regulation provides a comprehensive legal framework for the general requirements of electronic commerce,

[12] Jeane Neltje Saly et al., "Analisis Perlindungan Data Pribadi Terkait UU No. 27 Tahun 2022," *Jurnal Serina Sosial Humaniora* 1, no. 3 (October 2023): 145–53. https://journal.untar.ac.id/index.php/JSSH/article/view/28615

e-commerce operations, contract processing, and personal data protection, significantly shaping the legal landscape of Indonesia's digital economy.

Additionally, Presidential Regulation No. 47 of 2023 on the National Cyber Security Strategy and Cyber Crisis Management addresses some key aspects of cybersecurity. This regulation includes adaptive and innovative measures to safeguard all levels of cyberspace and its information assets from cyber threats and attacks. The National Cyber Security Strategy outlines the national policy direction for utilizing cyber resources to protect and promote national interests. Cyber Crisis Management regulates the effective management of resources and handling measures before, during, and after a cyber crisis. Focus areas in this regulation include governance, risk management, preparedness, protection of vital information infrastructure, national cryptographic independence, and international cooperation. This regulation aims to realize cybersecurity, protect the national digital economy ecosystem, and support the creation of a safe and responsible global cyberspace.

In particular, the National Cyber and Crypto Agency known as BSSN as one of the institutions engaged in digital and cyber also has several regulations related to cybersecurity. BSSN Regulation Number 8 of 2020 mainly regulates the scope of the implementation of public scope electronic systems and the implementation of private scope electronic systems, self-assessment processes and electronic system categories, Information Security Management System operators, guidance and supervision, and sanctions. Then, BSSN Regulation Number 10 of 2020 which regulates the implementation of cyber incident response teams, types and tasks, along with the services provided.

There are quite a lot of cybersecurity-related arrangements in Indonesia, but does that indicate good cyber protection? Indeed, the more regulations that govern, the less room there will be for cybercrime to occur which will hinder the growth of the digital economy. However, in the case of Indonesia, these regulations are not integrated to support each other between regulations and tend to regulate sectorally.[13] This fragmentation of the way it is regulated will usually cause confusion in cyber law enforcement itself. The problem of fragmentation of legal arrangements will result in law enforcement itself, problems such as consistency and standards in law enforcement. With many legal arrangements that do not support each other will cause many variations in the laws applied and enforced, which will create legal uncertainty and hinder law enforcement efforts.

In enforcement, fragmented legal arrangements will encourage more subjective law enforcement. This leads to discretionary law enforcement, where law enforcement is conducted on a casuistic basis instead of following clear, transparent, and uniform rules, the official has the freedom to determine what action to take.[14] For example, there is still often uncertainty about cyber law enforcement because the limits are sometimes still broken. Problems such as attacks in the banking sector, data theft, digital-based illegal trade, fraud to pornography are still sometimes confused whether they are handled with cyber regulations because they use digital media or whether they are handled with the Criminal Code.[15]

This fragmentation is also related to the authority of the institution tasked with maintaining cybersecurity itself. Due to this fragmentation, the lack of regulatory schemes and legal umbrellas causes authority between agencies to be divided and uncoordinated.[16] This leads to possible conflicts of authority between institutions. For example, BSSN and Kemenkominfo, Kemenkominfo and BSSN have authority related to information security and protection, but the scope of authority of both is not always clearly separate. This overlap can lead to conflicts over who is in charge of certain matters or who has higher jurisdiction in dealing with an issue. The

[13] Rosadi and Pratama, "Urgensi Perlindungan Data Pribadi Dalam Era Ekonomi Digital Di Indonesia."

[14] Ira Aprilianti and Siti Dina, "Co-Regulating the Indonesian Digital Economy" (Jakarta, Indonesia, 2021). https://www.cips-indonesia.org/publications/co-regulating-the-indonesian-digital-economy?lang=id

[15] Adji Saputra, Kristiawanto Kristiawanto, and Mohamad Ismed, "Rekonstruksi Penegakan Hukum Tindak Pidana Siber Di Indonesia," *SEIKAT: Jurnal Ilmu Sosial, Politik Dan Hukum* 3, no. 1 (February 9, 2024): 63–70, https://doi.org/10.55681/seikat.v3i1.1186.

[16] Noor Anjani, "Cybersecurity Protection in Indonesia" (Jakarta, Indonesia, 2021), https://doi.org/10.35497/341779. p. 5.

Ministry of Communication and Information oversees the regulation and supervision of the extensive use of information and communication technology, including aspects related to infrastructure, telecommunications, media, and internet services. Meanwhile, BSSN is tasked with safeguarding cybersecurity and addressing cyber threats.

The authority of BSSN is also focused on the use of the internet, which is related to security and information protection.[17] Previously, the Ministry of Communication and Information held authority over information security, internet protocol-based telecommunications networks, and network and telecommunications infrastructure. However, with the establishment of BSSN, these responsibilities have shifted to BSSN.[18] Thus, BSSN now oversees all forms of telecommunications that use the internet. Given that most telecommunications rely on the internet, this creates a jurisdictional overlap with the Ministry of Communication and Information, which is also involved in telecommunications and informatics. This overlap has led to a conflict of authority between the Ministry and BSSN.

The conflict of authority between BSSN and the Ministry of Communication and Information is only one of several possible conflicts of authority between institutions that occur due to unclear, sectoral, and fragmented legal arrangements related to cybersecurity that cause uncertain and uncoordinated cyber security efforts. Moreover, in handling cyber threats, actions are needed that are not only reactive to cyber threats but also proactive in dealing with weaknesses in existing cyber systems.

There are also problems from jurisdictions in order to realize cybersecurity in Indonesia. Because it utilizes digital technology, so many cybersecurity threats that occur in Indonesia are carried out by actors operating abroad. This jurisdictional issue will be complicated because of course there will be uncertainty about which law will be used or who has the authority to try a case due to international jurisdictional restrictions.[19] So, if there is no cooperation between Indonesia and other country in terms of handling this cyber threat, then it is possible that the perpetrators of cyber crimes can move freely without worrying about the consequences of their actions. Because it cannot be denied, that this cyber crime is a crime that crosses national borders.

Of course, the cybersecurity problems in Indonesia that have been described are only related to the legal landscape. Outside of the legal landscape, there are other issues that will certainly have a major impact on cybersecurity in Indonesia. Call it, problems such as infrastructure and the capabilities of the parties related to cybersecurity itself. However, that is another discussion outside this legal landscape, but at least it provides an idea of the complexity of a country's cybersecurity mechanisms.

3.2. Indonesia Cyber Law Development to Support Digital Economy Integration

When discussing the ASEAN digital economy, it cannot be separated from how Indonesia's potential in the digital economy itself. Based on data from e-Conomy 2024[20], the valuation of the digital economy in Indonesia has experienced a growth of 13% with a GMV of 90 billion USD which is expected to increase more than 200% in 2030 with a GMV valuation of 200-369 billion USD, and is also the largest in Southeast Asia. This is not strange considering that in 2024 there

[17] Hidayat Chusnul Chotimah, "Tata Kelola Keamanan Siber Dan Diplomasi Siber Indonesia Di Bawah Kelembagaan Badan Siber Dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]," *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional* 10, no. 2 (November 25, 2019): 113–28, https://doi.org/10.22212/jp.v10i2.1447. p. 124.

[18] IGN Mantra, "Tumpang Tindih Tugas Badan Siber Dengan Lembaga Lain," KOMINFO, August 26, 2020, https://www.komdigi.go.id/berita/sorotan-media/detail/tumpang-tindih-tugas-badan-siber-dengan-lembaga-lain.

[19] Fadhila Rahman Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia," *AL-BAHTS: Jurnal Ilmu Sosial, Politik, dan Hukum* 2, no. 1 (January 11, 2024): 8–16, https://doi.org/10.32520/albahts.v2i1.3044. p. 13.

[20] Google, Temasek, and Bain & Company, "E-Conomy SEA 2024," 2024, https://economysea.withgoogle.com/intl/id_id/home/.

are 221 million people who use the internet in Indonesia[21]. With such a large number of internet users, it is not impossible for Indonesia's digital share to make a major contribution to the digital economy in Indonesia. Moreover, trading through electronic systems or the internet enhances customer participation, leading to greater interaction among commercial sector participants that was previously limited to a global scale.[22] However, as the digital economy grows and more internet users engage with each other, the risk of cyber threats also increases.

To overcome these possible cyber threats, it is necessary to make legal regulatory efforts that can help provide security from the implementation of the digital economy in Indonesia. This legal regulation is also not only an effort to overcome cyber threats, but can also be used as a guideline and direction for parties to be able to form a secure cyber environment that can help integrate the digital economy. In relation to legal regulatory efforts to establish a secure cyber environment for the implementation of the digital economy, there are several things that need attention.

3.2.1. Sectoral and Fragmented Legal Arrangements

It has been explained in the previous section, that regulations related to cybersecurity are still sectoral or fragmented and there are also several points that need to be regulated further. This sectoral legal arrangement causes the implementation of cybersecurity to be confusing and can cause conflicts between institutions. The practice of implementing cybersecurity in Indonesia on a national scale is fragmented in various ministry and institutions.[23] As explained earlier, the Ministry of Communication and Information and BSSN overlap authority in cyber security efforts because the authority arrangements between the two are very close and it tends to be difficult to see the boundary between the authority of the two institutions. This happens because in addition to sectoral arrangements, there are also no positive laws governing cybersecurity.[24]

In addition, this sectoral legal arrangement has also led to partial implementation of the law in various sectors. Because this digital economy is interrelated with each other in various sectors which then meet with digital platforms. In e-commerce alone there are many regulations that are interrelated and tied to various institutions and due to different sector arrangements so that they cannot be applied comprehensively in digital platforms, such as Law Number 7 of 2014 concerning Trade (authorization of the Ministry of Trade), Law Number 10 of 1998 concerning Banking (authorization of Bank Indonesia), Law Number 25 of 2007 concerning Capital Investment (authorization of the Indonesia Investment Coordinating Board), Law Number 20 of 2008 concerning MSMEs (authorization at the Ministry of Cooperatives and SMEs), Minister of Finance Regulation Number 112 of 2018 (authorization at the Ministry of Finance), Law Number 38 of 2009 concerning Post, and Law Number 19 of 2016 concerning ITE (authorization at the Ministry of Communication and Information).[25] Thus, if there is no arrangement that can regulate the relationship between institutions in the implementation of the digital economy, it will be very likely that there will be conflicts of authority between these institutions. On the other hand, the many legal arrangements on an aspect of the digital economy will cause confusion in terms of law enforcement later.

This confusion in law enforcement is still related to the meeting of certain regulations in terms of the implementation of the digital economy. When faced with problems such as fraud in trading through digital platforms, fraud has clearly been regulated in the Criminal Code, but in this

---

21 APJII, "APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang."

22 Muhamad Rizal, Sinta Dewi Rosadi, and Agus Taryana, "Legal Framework for Consumer Data Protection For Digital Business SMES in Indonesia," *Journal of Law and Sustainable Development* 12, no. 1 (January 31, 2024): e2809, https://doi.org/10.55908/sdgs.v12i1.2809. p. 18.

23 Sarah Safira Aulianisa and Indirwan Indirwan, "Critical Review of the Urgency of Strengthening the Implementation of Cyber Security and Resilience in Indonesia," *Lex Scientia Law Review* 4, no. 1 (May 8, 2020): 33–48, https://doi.org/10.15294/lesrev.v4i1.38197. p. 42.

24 *Ibid.*

25 Vience Mutiara Rumata and Ashwin Sasongko Sastrosubroto, "The Paradox of Indonesian Digital Economy Development," in E-Business - Higher Education and Intelligence Applications (IntechOpen, 2021), https://doi.org/10.5772/intechopen.92140. p. 8.

case because the fraud is carried out by means of electronic transactions, it means that it can also be handled using the ITE Law. When faced with such a situation, there will be confusion in law enforcement, because each arrangement is linked to each other. In the end, this leads to legal uncertainty, and makes law enforcement ineffective and inefficient.

3.2.2. The Weakness of Indonesia Cyber Law

There are two things that need to be considered when discussing cyber law that is still not strong, namely, jurisdictional regulations that are still weak [26] and lack of regulations that specifically regulate cyber itself[27]. The implementation of the digital economy is carried out in cyberspace that knows no borders. Because of this, transaction activities do not only occur domestically, but also transcend national borders.[28] This causes the digital economy market in Indonesia will also be exposed to cyber threats from abroad, but on the other hand when it gets cyber threats from abroad, Indonesia will face difficulties to carry out law enforcement against cyber criminals from abroad. Because Indonesia's jurisdiction is unable to prosecute cyber criminals who are abroad. Although Indonesia's ITE Law provides for extraterritorial application against cybercrimes that harm national interests, its enforcement remains weak. Despite this normative scope, authorities often face major challenges in identifying, investigating, and prosecuting cross-border offenders. The issue lies not in the legal basis itself, but in the lack of effective international cooperation, procedural harmonization, and enforcement infrastructure.[29] As a result Indonesia remains exposed to transnational cyber threats, and a significant gap persists between the law's intent and the government's practical enforcement capabilities in a borderless digital economy.

It is clear that Indonesia cannot make a unilateral regulation which is then used as a basis for prosecuting foreign cyber criminals who threaten Indonesia, which is why it is necessary for Indonesia to conduct cyber diplomacy with other countries in order to overcome cross-border cyber threats.[30] At the same time together with other countries and related parties to form a joint regulation that regulates relations between countries in the context of law enforcement to overcome cyber threats. Because with the establishment of legal arrangements between countries, this will be a strong driver in improving security and connectivity in the digital economy ecosystem. [31]

Another problem is the lack of specific cyber regulation. Cybercrime is a very dynamic and rapidly evolving crime, often faster than the development of the rule of law. As a result, existing laws may not have clear enough provisions or definitions to deal with emerging or complex types of cybercrime. Especially if from the beginning there are no arrangements related to cyber crime itself. Even existing cyber-related arrangements are outdated and cannot be used to regulate the digital economy sector[32]. Even though the development of cyberspace occurs very quickly and needs to continue to be developed every time.

---

[26] Rahman Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia."

[27] Muhamad Rizal and Yanyan Yani, "Cybersecurity Policy and Its Implementation in Indonesia," *JAS (Journal of ASEAN Studies)* 4, no. 1 (August 9, 2016): 61, https://doi.org/10.21512/jas.v4i1.967. p. 70.

[28] Rizal, Rosadi, and Taryana, "Legal Framework for Consumer Data Protection For Digital Business SMES in Indonesia." p. 15.

[29] Saputra, Kristiawanto, and Ismed, "Rekonstruksi Penegakan Hukum Tindak Pidana Siber Di Indonesia." p. 69.

[30] Chotimah, "Tata Kelola Keamanan Siber Dan Diplomasi Siber Indonesia Di Bawah Kelembagaan Badan Siber Dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]." p. 123

[31] Lurong Chen, *Improving Digital Connectivity for E-Commerce: A Policy Framework and Empirical Note for ASEAN*, ERIA Discussion Paper Series (Economic Research Institute for ASEAN and East Asia, 2020).

[32] Mutiara Rumata and Sasongko Sastrosubroto, "The Paradox of Indonesian Digital Economy Development." p, 7.

In the existing cyber-related arrangements, they are still unable to provide specific clarity regarding cyber crime[33], for example, the regulations regarding interference systems and system sabotage have not been properly regulated and specific. In the ITE Law, regulations related to system interference and system sabotage only exist in Article 30 and Article 33, even though regulations regarding interference and sabotage actions still cannot be explained concretely and specifically. Meanwhile, in cyber law arrangements, it is important to make specific and concrete legal arrangements. Thus, the regulation must clearly mention and dissect all forms of cyber threats and cybercrime.[34] Cyber law arrangements also need to clarify which are the boundaries of private and public.[35] This is to ensure the privacy rights of individuals can be well maintained, and clearly provide limits for individuals and related parties in acting in the digital space.

3.3. Indonesia Cyber Law Development to Support Digital Economy Integration

The explosion of digital technology has placed powerful tools in the hands of ordinary citizens, but these tools can also be used to inflict significant harm. Cybercriminals can now wreak havoc on individuals, companies, and governments from anywhere in the world with minimal cost. While traditional laws often apply online, the nature of cybercrime and the difficulty of gathering evidence necessitate unique legal solutions. To effectively deal with the evolving nature of cybercrime, Indonesia must look beyond its current legal framework and explore adaptive strategies from more established systems. The United States, for example, offers a model of integrated legal, institutional, and international approaches to combating cyber threats. Learning from the U.S. experience can help Indonesia strengthen its legal instruments and enforcement capacity, particularly in dealing with transnational cybercrimes. This comparative insight is crucial in shaping a modern, responsive cyber law regime that aligns with today digital realities.[36]

Traditional legal systems, designed for a physical world, struggle to address the realities of cybercrime. [37] These established laws define criminal behavior, but they haven't kept pace with the technological advancements that empower cybercriminals. These criminals exploit the borderless nature of cyberspace to launch attacks and commit fraud, inflicting significant costs on individuals, businesses, and governments. The damage can be multifaceted from data breaches and financial losses to reputational harm and infrastructure destruction. The potential for widespread devastation across multiple countries simultaneously necessitates a modern legal framework specifically designed to combat cybercrime in this new digital age.

The digital revolution, fueled by ever-evolving technology and global connectivity, has fundamentally reshaped our world. It's not just about economic growth it's about empowering individuals and societies. Digital tools have democratized information and education, expanded access to crucial services, and created new markets for businesses to thrive globally. Citizens are more engaged, governments are more transparent, and the very fabric of civic life has been transformed by this digital wave.[38]

The future holds immense promise thanks to the ongoing advancements in digital technology. These tools can be harnessed to tackle some of humanity's most pressing challenges: climate change, economic disparity, and global health crises. While the digital revolution offers a bright future, it's not without its shadows. The global competition for dominance in cyberspace raises security concerns. Malicious actors, both state and non-state, threaten critical infrastructure, essential services, and even individuals. Crime flourishes in the digital realm, fueled by readily available tools and the vast amount of personal information readily

[33] Rizal and Yani, “Cybersecurity Policy and Its Implementation in Indonesia.”
[34] Rizal and Yani, “Cybersecurity Policy and Its Implementation in Indonesia.”
[35] Anjani, “Cybersecurity Protection in Indonesia.” p. 6.
[36] Zeinab Karake Shalhoub and Sheika Lubna Al-Qasimi, Cyber Law and Cyber Security in Developing and Emerging Economies (Massachusetts: Edgar Elgar Publishing, 2010). p. 1
[37] Shalhoub and Al-Qasimi, “Cyber Law and Cyber Security in Developing and Emerging Economies.” p.2
[38] U.S. Department of State, “United States International Cyberspace & Digital Policy Strategy,” U.S. Department of State, July 18, 2024, https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/.

available online. These challenges paint a complex picture, demanding innovative solutions to ensure the benefits of technology outweigh the risks.[39]

In response to increasingly complex cyber threats, the United States has adopted a multi-layered strategy that combines legal innovation, public-private collaboration, and international engagement.[40] U.S. approach fostering a secure digital ecosystem by supporting competition, consumer choice, and private sector involvement. The government actively partners with technology actors to shape policy directions, as reflected in frameworks like the EU–U.S. Data Privacy Framework and the OECD Declaration on Trusted Government Access to Data. [41] These initiatives promote data protection while enabling secure global data flows. The 2023 Executive Order on Artificial Intelligence further exemplifies this commitment by establishing new standards for safety, privacy, and ethical deployment through cooperation with industry and civil society. In enforcement, the U.S. has implemented concrete actions through transnational operations and partnerships aimed at dismantling cybercrime infrastructure. The Budapest Convention, which the U.S. supports, sets out binding standards for criminalizing cyber offenses and enhancing international cooperation. Together, these efforts demonstrate a coordinated model where regulatory clarity, cross-sectoral engagement, and proactive law enforcement converge. Indonesia, while facing similar digital vulnerabilities, could benefit from adapting such an approach to cultivate a more agile and resilient digital governance framework tailored to its national context.

Many countries address cyber security risks through both privacy and critical infrastructure legislation. The European Union demonstrates a dual regulatory approach to cybersecurity through the General Data Protection Regulation and the Network and Information Systems Directive, focusing respectively on personal data protection and the security of critical infrastructure. The GDPR, in force since 2018, obliges organizations to adopt technical and organizational measures to prevent unauthorized access and ensure data integrity. Article 32, for example, mandates regular testing and evaluation of security mechanisms. This framework has led to notable improvements in cybersecurity readiness. A 2019 RSM study found that 75% of UK companies increased their cybersecurity investments due to GDPR, while a separate 2020 UK study reported that 82% of organizations enhanced their cyber measures.[42] These outcomes reflect how robust privacy obligations can strengthen both individual rights and systemic resilience. Moreover, the GDPR has spurred wider adoption of encryption, penetration testing, and risk management practices. As such, the European model offers a relevant reference for Indonesia in developing integrated cyber regulations aligned with the realities of an increasingly digitized and threat-prone environment.

Australia has also taken concrete regulatory steps to confront growing cyber threats, significant progress has been made in improving the cyber resilience of businesses through both institutional collaboration and regulatory reforms. Financial institutions are subject to Prudential Standard CPS 234 on Information Security, requiring proportionate risk-based controls. The Privacy Act 1988 especially Australian Privacy Principle 11 and its Notifiable Data Breaches scheme obligate organizations to prevent unauthorized access and report breaches. [43] Additionally, Section 912A of the Corporations Act 2001 mandates licensees to maintain adequate risk management systems, extended to cybersecurity responsibilities. This was tested in the case of ASIC v RI Advice Group, [44] where insufficient cybersecurity governance was legally challenged. These legislative developments reflect Australia's evolving approach to

[39] U.S. Department of State, “United States International Cyberspace & Digital Policy Strategy.”
[40] U.S. Department of State, “United States International Cyberspace & Digital Policy Strategy,”
[41] U.S. Department of State, “United States International Cyberspace & Digital Policy Strategy.” p. 31
[42] RSM UK, “Impact of GDPR on Cyber Security Outcomes” (London, 2020), https://assets.publishing.service.gov.uk/media/5f294433d3bf7f1b18aaad27/Impact_of_GDPR_on_cyber_security_outcomes.pdf.
[43] Department of Home Affairs, *Strengthening Australia’s Cyber Security Regulations and Incentives* (Commonwealth of Australia, 2020), https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australia-cyber-security-regulations-discussion-paper.pdf. p. 14
[44] Department of Home Affairs, “Strengthening Australia’s Cyber Security Regulations and Incentives” p. 13

embedding cybersecurity as an integral component of corporate responsibility. This ensures that those at the helm of Australian businesses are equipped with the knowledge and skills necessary to effectively manage cyber threats. By fostering collaboration, providing resources, and promoting leadership awareness, Australia is making significant strides toward a more secure digital environment.

Australia is also taking steps to strengthen its cyber security framework through new regulations. The Security Legislation Amendment (Critical Infrastructure) Bill 2020 introduces mandatory cyber security incident reporting for critical infrastructure. This bill also requires enhanced cyber security obligations for "systems of national significance" assets deemed most critical to the nation's security. Additionally, boards overseeing critical infrastructure will be required to approve risk management programs as part of their legal obligations. The Australian Prudential Regulation Authority has also implemented its prudential standard CPS 234: Information Security. This standard, which came into effect in 2019, mandates that banks, insurers, and superannuation funds take specific measures to ensure resilience against information security threats. These regulatory advancements demonstrate Australia's multi-pronged approach to cyber security, combining collaboration, education, and legal requirements to create a more secure digital landscape for businesses and citizens alike.[45]

3.4. Possible Solution For Indonesia Cyber Law

Indonesia's booming digital economy demands a legal framework that balances growth with security. There are several efforts and approaches that can address the chaotic problem of legal arrangements and conflicts of authority in the implementation of the digital economy. One option is to revise existing regulations to provide clarity on institutional authority. For example, clarifying the roles of the Ministry of Communication and Information and BSSN can prevent conflicts. Furthermore, changes related to the authority of this institution can later also focus on strengthening coordination between related institutions. This change can also be done to make the substance of existing legal regulations so that they can be in harmony with each other in relation to the implementation of the digital economy, even though each regulation has a different regulatory substance. However, if each related regulation leads to the same regulatory direction, it will form a harmony that can improve the performance of each existing regulation.

Another option is the establishment of new regulations specifically tailored to govern the digital economy. A specialized regulation could harmonize all aspects related[46] to digital transactions, cybersecurity, and other elements of the digital space. This could involve creating entirely new legislation or integrating provisions into a comprehensive cyber law that unifies existing statutes like the Job Creation Law and the Law on Harmonization of Tax Regulations. A unified regulatory framework would help industries realize economies of scale and foster digital economic growth.

Furthermore, there is a pressing need for more specific regulations addressing cyber threats and cybercrime. These regulations should provide technical standards for cybersecurity, ensuring comprehensive protection against evolving risks. Developing new legislation that both introduces fresh cyber policies and harmonizes existing regulations would offer a robust legal foundation for a secure digital environment. With efforts to understand international best practices, Indonesia can draw inspiration from advanced countries' experiences in integrating cyber law into digital economy development.

Emulating the dual regulatory models of the European Union and Australia, Indonesia could adopt a two-pronged strategy to enhance both individual rights and systemic cybersecurity resilience. A data privacy framework modeled after the EU's General Data Protection Regulation would safeguard citizens' digital rights and promote accountability, while regulatory measures inspired by Australia's Security of Critical Infrastructure Bill could protect critical sectors which in this context is digital economy from escalating cyber threats. However, Indonesia's current

[45] Department of Home Affairs, "Strengthening Australia's Cyber Security Regulations and Incentives"

[46] Syahlan, "Effective and Efficient Synchronization in Harmonization of Regulations Indonesia," *Journal of Human Rights, Culture and Legal System* 1, no. 1 (March 30, 2021), https://doi.org/10.53955/jhcls.v1i1.7. p. 56.

Personal Data Protection Law remains primarily administrative in nature. While it borrows principles from the GDPR, such as consent and purpose limitation, it lacks substantive provisions concerning users' digital rights and clear technical standards on encryption, breach response, and systemic risk governance. Article 35 mandates organizational safeguards, but without detailed benchmarks akin to GDPR Article 32, the protection remains shallow. To close this gap, Indonesia must move beyond formal alignment and build a regulatory framework that integrates cybersecurity obligations, articulates substantive rights, and facilitates international cooperation. Drawing from practices in the United States, including cross-sector enforcement initiatives and bilateral legal instruments like the Budapest Convention, Indonesia can establish a more adaptive and enforceable data governance system aligned with the realities of transnational cyber threats.

Collaboration between government agencies, intelligence services, and the private sector, complemented by educational initiatives for business leaders, would strengthen this approach. A complete overhaul of Indonesia's existing cyber law framework may not be necessary. Instead, a thorough analysis can identify targeted amendments to address evolving cyber threats while fostering a business-friendly environment. The United States' focus on competition, consumer choice, and a dynamic private sector also provides valuable lessons for Indonesia. The key lies in striking a balance between fostering innovation and ensuring security through effective enforcement, public awareness campaigns, and continuous regulatory adaptation. By following these steps, Indonesia can create a secure and trustworthy digital space that fuels economic growth without stifling entrepreneurial spirit.

4. Conclusion

Indonesia holds significant potential in the digital economy, positioning itself as a leader in Southeast Asia in this domain. The rapid growth of digital technologies and the expanding role of e-commerce, fintech, and online services have solidified Indonesia's status as a hub for digital economic activities. However, this tremendous potential has not been fully realized due to inadequate cyber law arrangements that fail to address the complexities of the digital landscape. A robust legal framework is crucial for the seamless integration of the digital economy, as it fosters trust, attracts investors, and encourages greater participation from users in digital transactions. Without clear and effective regulations, the full benefits of the digital economy cannot be harnessed.

The current cybersecurity regulations in Indonesia remain fragmented and sector-specific, which results in overlapping jurisdictions between regulatory bodies and institutions. This lack of coordination hampers effective governance and creates confusion regarding the roles and responsibilities of various entities. The absence of a comprehensive legal framework further complicates law enforcement, as there are unclear lines of authority when it comes to cybersecurity enforcement. Laws related to cyber activities and the digital economy are often vague, and enforcement agencies struggle to address cross-border cyber threats due to insufficient jurisdictional regulations and limited international cooperation. This gap in the legal framework poses a serious risk to the protection of critical digital infrastructure and personal data, undermining public trust in the digital environment.

To address these issues, it is crucial to revise and update existing regulations to clearly define the authority of institutions responsible for cybersecurity. A more cohesive regulatory approach would help streamline the responsibilities of various agencies, ensuring better coordination and more effective law enforcement. Additionally, there is a pressing need for new regulations specifically designed to protect the digital economy and address the unique challenges posed by cybersecurity threats. These regulations must be integrated into the existing legal framework, harmonizing with laws concerning privacy, data protection, and digital commerce. By establishing clear technical standards for cybersecurity, the country can build a more resilient digital ecosystem capable of defending against emerging threats.

Indonesia can also benefit from studying the experiences of other regions with advanced digital economies. For example, the European Union's General Data Protection Regulation (GDPR) offers valuable lessons in data privacy and security, providing a solid legal foundation for protecting users' personal information. Similarly, Australia's Critical Infrastructure Bill

demonstrates the importance of safeguarding essential digital assets, ensuring that critical systems are protected from cyber attacks. Adopting a dual approach, where both data privacy and the security of critical digital infrastructure are prioritized, would be an effective strategy for Indonesia.

In addition to legislative reforms, collaboration between government agencies, intelligence services, and the private sector is crucial for a comprehensive cybersecurity strategy. Public-private partnerships can foster innovation while ensuring that adequate security measures are in place. Furthermore, public awareness campaigns and education initiatives are vital to empowering individuals and organizations to take responsibility for their own cybersecurity. By raising awareness about the importance of cybersecurity and providing the necessary tools and knowledge, Indonesia can create a culture of security that permeates all sectors of society.

Acknowledgement

The authors sincerely thank the reviewers for their valuable contributions in enhancing and refining the quality of this work. Appreciation is also extended to all the lecturers in the Master of Laws Program at Hasanuddin University, as well as the supporting research teams, for their unwavering support and encouragement in advancing this study, particularly in the field of Indonesian legal studies, with a special focus on Cyber Law.

Funding Information

None

Conflicts of Interest Statement

The authors declare that there is no conflict of interest regarding the publication of this article.

References

Anjani, Noor. “Cybersecurity Protection in Indonesia.” Jakarta, Indonesia, 2021. https://doi.org/10.35497/341779.

APJII. “APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang.” Asosiasi Penyelenggara Jasa Internet Indonesia, February 7, 2024. apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang.

Aprilianti, Ira, and Siti Dina. “Co-Regulating the Indonesian Digital Economy.” Jakarta, Indonesia, 2021. https://www.cips-indonesia.org/publications/co-regulating-the-indonesian-digital-economy?lang=id.

Aulianisa, Sarah Safira, and Indirwan Indirwan. “Critical Review of the Urgency of Strengthening the Implementation of Cyber Security and Resilience in Indonesia.” *Lex Scientia Law Review* 4, no. 1 (May 8, 2020): 33–48. https://doi.org/10.15294/lesrev.v4i1.38197.

Berg, Bibi van den, and Esther Keymolen. “Regulating Security on the Internet: Control versus Trust.” *International Review of Law, Computers & Technology* 31, no. 2 (May 4, 2017): 188–205. https://doi.org/10.1080/13600869.2017.1298504.

Chen, Lurong. *Improving Digital Connectivity for E-Commerce: A Policy Framework and Empirical Note for ASEAN*. ERIA Discussion Paper Series. Economic Research Institute for ASEAN and East Asia, 2020.

Chotimah, Hidayat Chusnul. “Tata Kelola Keamanan Siber Dan Diplomasi Siber Indonesia Di Bawah Kelembagaan Badan Siber Dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency].” *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional* 10, no. 2 (November 25, 2019): 113–28. https://doi.org/10.22212/jp.v10i2.1447.

Dahlman, Carl, Sam Mealy, and Martin Wermelinger. “Harnessing the Digital Economy for Developing Countries.” Paris, December 2016. https://doi.org/10.1787/4adffb24-en

Department of Home Affairs. *Strengthening Australia’s Cyber Security Regulations and Incentives*. Commonwealth of Australia, 2020. https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australia-cyber-security-regulations-discussion-paper.pdf.

Google, Temasek, and Bain & Company. “E-Conomy SEA 2024,” 2024. https://economysea.withgoogle.com/intl/id_id/home/.

Kominfo Newsroom. “Indonesia Controls 40 Percent of ASEAN Digital Economy Market.” ASEAN Indonesia 2023, August 14, 2023. asean2023.id/en/news/indonesia-controls-40-percent-of-asean-digital-economy-market.

Mantra, IGN. “Tumpang Tindih Tugas Badan Siber Dengan Lembaga Lain.” KOMINFO, August 26, 2020. https://www.komdigi.go.id/berita/sorotan-media/detail/tumpang-tindih-tugas-badan-siber-dengan-lembaga-lain.

Mutiara Rumata, Vience, and Ashwin Sasongko Sastrosubroto. “The Paradox of Indonesian Digital Economy Development.” In *E-Business - Higher Education and Intelligence Applications*. IntechOpen, 2021. https://doi.org/10.5772/intechopen.92140.

Rahman Najwa, Fadhila. “Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia.” *AL-BAHTS: Jurnal Ilmu Sosial, Politik, dan Hukum* 2, no. 1 (January 11, 2024): 8–16. https://doi.org/10.32520/albahts.v2i1.3044.

Rizal, Muhamad, Sinta Dewi Rosadi, and Agus Taryana. “Legal Framework for Consumer Data Protection For Digital Business SMES in Indonesia.” *Journal of Law and Sustainable Development* 12, no. 1 (January 31, 2024): e2809. https://doi.org/10.55908/sdgs.v12i1.2809.

Rizal, Muhamad, and Yanyan Yani. “Cybersecurity Policy and Its Implementation in Indonesia.” *JAS (Journal of ASEAN Studies)* 4, no. 1 (August 9, 2016): 61. https://doi.org/10.21512/jas.v4i1.967.

Rosadi, Sinta Dewi, and Garry Gumelar Pratama. “Urgensi Perlindungan Data Pribadi Dalam Era Ekonomi Digital Di Indonesia.” *Veritas et Justitia* 4, no. 1 (2018). https://doi.org/10.25123/vej.v4i1.2916

Rosadi, Sinta Dewi, and Zahra Tahira. “Consumer Protection in Digital Economy Era: Law in Indonesia.” *Yustisia* 7, no. 1 (2018). https://doi.org/10.20961/yustisia.v7i1.20144

RSM UK. “Impact of GDPR on Cyber Security Outcomes.” London, 2020. https://assets.publishing.service.gov.uk/media/5f294433d3bf7f1b18aaad27/Impact_of_GDPR_on_cyber_security_outcomes.pdf.

Saly, Jeane Neltje, Halena Artamevia, Kendelif Kheista, Barnabas Juni Saputra Gulo, Evellyn Abigael Rhemrev, and Michelle Christie. “Analisis Perlindungan Data Pribadi Terkait UU No. 27 Tahun 2022.” *Jurnal Serina Sosial Humaniora* 1, no. 3 (October 2023): 145–53. https://journal.untar.ac.id/index.php/JSSH/article/view/28615

Saputra, Adji, Kristiawanto Kristiawanto, and Mohamad Ismed. “Rekonstruksi Penegakan Hukum Tindak Pidana Siber Di Indonesia.” *SEIKAT: Jurnal Ilmu Sosial, Politik Dan Hukum* 3, no. 1 (February 9, 2024): 63–70. https://doi.org/10.55681/seikat.v3i1.1186.

Shalhoub, Zeinab Karake, and Sheika Lubna Al-Qasimi. *Cyber Law and Cyber Security in Developing and Emerging Economies*. Massachusetts: Edgar Elgar Publishing, 2010.

Soekanto, Soerjono. *Pengantar Penelitian Hukum*. Jakarta: Universitas Indonesia, 1989.

Suryati, Layang Sardana, Ramanata Disurya, and Yanuar Syam Putra. “Penguatan Literasi Digital Dalam Pencegahan Pelanggaran Hukum Siber (Cyber Law).” *Wajah Hukum* 8, no. 1 (2024): 84–94. http://dx.doi.org/10.33087/wjh.v8i1.1447

Syahlan. “Effective and Efficient Synchronization in Harmonization of Regulations Indonesia.” *Journal of Human Rights, Culture and Legal System* 1, no. 1 (March 30, 2021). https://doi.org/10.53955/jhcls.v1i1.7.

U.S. Department Of State. “United States International Cyberspace & Digital Policy Strategy.” U.S. Department Of State , July 18, 2024. https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/.