Journal Widya Gama Law Review
Faculty of Law, Universitas Widya Gama Malang
Vol 2, No 1 (2025): April, Page 67-84

e-ISSN: 3063-8275

Comparison of Criminal Provisions on Cybercrime In Indonesia and Singapore

Ferlina Mutiara Farah

Faculty of Law, Universitas Widya Gama Malang, ferlina61@gmail.com

Halimatus Khalidawati Salmah

Faculty of Law, Universitas Widya Gama Malang, hkhsalmah@widyagama.ac.id

ABSTRACT

This article compares the cyber law frameworks of Indonesia and Singapore, two key Southeast Asian countries in the digital era. Using a normative juridical and comparative approach, the study analyzes similarities and differences in the regulation and implementation of cyber laws, focusing on the scope of cybercrime, procedures for digital evidence, personal data protection, and international cooperation. The findings show that Singapore adopts a more integrated and risk-based approach, particularly in personal data protection and critical infrastructure security, while Indonesia's framework remains broader but less specific. Both countries face challenges in law enforcement and cross-border cooperation, but Singapore demonstrates more effective institutional coordination. The study recommends legal harmonization, capacity building, and enhanced regional collaboration to address evolving cyber threats in Southeast Asia. These insights contribute to the development of more robust and adaptive cyber law policies in the region.
Keywords: Comparison; Singapore; Indonesia; Legal System; Cyber Security

INTRODUCTION

The use of the Internet has fundamentally transformed people's lifestyles and cultures, particularly in the ways they learn, work, communicate, shop, and engage in various daily activities.[1] Nowadays, the Internet is increasingly utilized for communication purposes, such as through electronic mail (email) and social networking platforms, which are considered more effective and efficient than traditional means.[2] The digital era has brought significant progress to the socio-economic and political sectors across the globe, fostering new opportunities for innovation, economic growth, and social interaction.[3]

[1] Anonymous, "Cybersecurity Policy Making at a Turning Point," *OECD Digital Economy Papers*, no. 211 (2012): 0_1,2,4-56, http://search.proquest.com.library.capella.edu/docview/1223514107?accountid=27965%5Cnhttp://wv9lq5ld3p.search.serialssolutions.com.library.capella.edu/?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/ABI/INFORM+Global&rft_val_fmt=info:ofi/f.

[2] Jason R. C. Nurse et al., "Cybersecurity Awareness. In: Encyclopedia of Cryptography, Security and Privacy," *Kent University Repository*, 2021, 1–4.

[3] Dedy Obet, Suharto Suharto, and Henri Mujoko, "Cyber Cooperation in the Framework of the Asean Regime," *Jurnal Pertahanan: Media Informasi Ttg Kajian & Strategi Pertahanan Yang Mengedepankan Identity, Nasionalism & Integrity* 7, no. 2 (2021): 254, https://doi.org/10.33172/jp.v7i2.1264.

Journal Widya Gama Law Review
Faculty of Law, Universitas Widya Gama Malang
Vol 2, No 1 (2025): April, Page 67-84
e-ISSN: 3063-8275

However, it cannot be denied that the Internet also presents a range of negative impacts.[4] The proliferation of harmful content is widely reported in various media, including the spread of pornographic material, online gambling, fraud, harassment, defamation, fake news, and other illicit activities.[5] In addition, cyberbullying-often targeting children and teenagers-has become a growing concern.[6] The phenomenon of cybercrime has even resulted in major domestic websites being hacked, causing substantial losses and undermining public trust in digital platforms.[7]

To mitigate the risks of cybercrime, it is essential to emphasize fundamental principles that every Internet user must understand.[8] The ethical standards and norms that apply in the real world are equally relevant in cyberspace.[9] Therefore, healthy and safe Internet usage should be taught from an early age by instilling good Internet ethics (cyber ethics).[10] This education is crucial to prevent negative behaviors originating from the real world from spreading into the virtual world, which could then have adverse effects back in the real world.[11]

Raising awareness among the younger generation about both the opportunities and risks of the Internet is necessary, as is the active involvement of parents in supervising and guiding their children. Parental supervision can help protect children from exposure to harmful content and encourage them to engage in more creative and productive online activities.[12]

In Indonesia, Law Number 19 of 2016 concerning Electronic Information and Transactions (UU ITE) serves as a pivotal regulation governing the use and misuse of information and electronic technology.[13] The Electronic Information and Transactions establishes a comprehensive legal framework for electronic transactions, the dissemination of

[4] Kim Kwang Raymond Choo, "The Cyber Threat Landscape: Challenges and Future Research Directions," *Computers and Security* 30, no. 8 (2011): 719–31, https://doi.org/10.1016/j.cose.2011.08.004.
[5] Dadang Suhendi and Erwin Asmadi, "Cyber Laws Related to Prevention of Theft of Information Related to Acquisition of Land and Infrastructure Resources in Indonesia," *International Journal of Cyber Criminology* 15, no. 2 (2021): 135–43, https://doi.org/10.5281/zenodo.4766552.
[6] Iqbal Ramadhan, "Building Cybersecurity Regulation in Southeast Asia: A Challenge for the Association of Southeast Asian Nations (ASEAN)," *Journal of Social and Political Sciences* 3, no. 4 (2020), https://doi.org/10.31014/aior.1991.03.04.230.
[7] Susan W. Brenner, "Cybercrime: Criminal Threats from Cyberspace," *Cybercrime: Criminal Threats from Cyberspace*, 2010, 1–283, https://doi.org/10.5860/choice.48-0685.
[8] Nir Kshetri, *Cybercrime and Cybersecurity in the Global South* (GOVERNING GLOBAL PRODUCTION, 2013).
[9] "Council of Europe Convention on Cybercrime," n.d., https://www.coe.int/en/web/cybercrime/the-%0Abudapest-convention%0A.
[10] Samra Al Kandy, Tamrin Fathoni, and Arief Fahmi Lubis, "Evolution and Challenges of Cyber Law in the Digital Era : Case Studies in Developing Countries" 1, no. 1 (2024): 1–10.
[11] Association of Southeast Asian Nations, "ASEAN Cybersecurity Cooperation Strategy (2021-2025)," *Asean.Org*, 2022, 1–14, https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf.
[12] ASEAN Secretariat, "Badan Siber Dan Sandi Negara (BSSN)," n.d.
[13] Indonesia Republik, "UU ITE Nomor 19 Tahun 2016," Pub. L. No. 19, 44 Journal of Physics A: Mathematical and Theoretical 287 (2016), file:///C:/Users/Lenovo/Downloads/UU Nomor 19 Tahun 2016.pdf.

Journal Widya Gama Law Review
Faculty of Law, Universitas Widya Gama Malang
Vol 2, No 1 (2025): April, Page 67-84
e-ISSN: 3063-8275

digital information, and other aspects of social interaction in cyberspace.[14] Its primary objective is to create a secure digital environment by protecting the rights of individuals and organizations and by imposing sanctions for violations.[15] The Electronic Information and Transactions Law is broad in scope, covering various aspects ranging from electronic transactions and content distribution on the Internet to the protection of personal data.[16]

Despite its comprehensive coverage, the Electronic Information and Transactions Law adopts a general approach, providing a broad but sometimes ambiguous framework for regulating digital activities in Indonesia.[17] Recognizing the increasing complexity of the digital environment, both Indonesia and Singapore have developed specific (lex specialis) regulations to address particular aspects of technology, ensuring that requirements for security, privacy, and fairness are met.[18]

Globally, countries have established and implemented legal frameworks to safeguard their infrastructure and societies from the negative impacts of information technology.[19] These frameworks are designed not only to ensure the safe and responsible use of technology but also to address the legal challenges that arise from the rapid development of information and communication technology.[20] Indonesia and Singapore, as part of this global movement, continue to adapt and strengthen their legal systems to respond effectively to the evolving landscape of cyber threats.[21]

[14] Muhamad Rizal and Yanyan Yani, "Cybersecurity Policy and Its Implementation in Indonesia," *JAS (Journal of ASEAN Studies)* 4, no. 1 (2016): 61, https://doi.org/10.21512/jas.v4i1.967.
[15] Budi Kristian Bivanda Putra, "Kebijakan Aplikasi Tindak Pidana Siber (Cyber Crime) Di Indonesia," *Pamulang Law Review* 1, no. 1 (2019): 1, https://doi.org/10.32493/palrev.v1i1.2842.
[16] Fahlesa Munabari et al., "Cyber Espionage in Indonesia : Legal Challenges and The Role of Institutions in the Digital Era" 8 (2024): 109–31.
[17] the Union of Myanmar and the Kingdom of Thailand, "Treaty on Mutual Legal Assistance in Criminal Matters," *Sustainability (Switzerland)*, 2006, http://scioteca.caf.com/bitstream/handle/123456789/1091/RED2017-Eng-8ene.pdf?sequence=12&isAllowed=y%0Ahttp://dx.doi.org/10.1016/j.regsciurbeco.2008.06.005%0Ahttps://www.researchgate.net/publication/305320484_SISTEM_PEMBETUNGAN_TERPUSAT_STRATEGI_MELESTARI.
[18] Oecd, "Cybersecurity Policy Making at a Turning Point. Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy.," *Organisation for Economic Co-Operation and Development*, 2012, https://doi.org/http://dx.doi.org/10.1787/5k8zq92vdgtl-en.
[19] Access Partnership, "Norms For Cybersecurity in Southeast Asia: Policy Options for Collaborative Security in the Southeast Asian Region," 2017, 20, https://ccapac.asia/wp-content/uploads/2022/03/Norms-for-Cybersecurity-in-Southeast-Asia.pdf.
[20] Nikolas Ioannidis, "Personal Data Protection," *Border Control and New Technologies*, 2021, 61–80, https://doi.org/10.46944/9789461171375.4.
[21] Thailand, "Treaty on Mutual Legal Assistance in Criminal Matters."

Journal Widya Gama Law Review
Faculty of Law, Universitas Widya Gama Malang
Vol 2, No 1 (2025): April, Page 67-84
e-ISSN: 3063-8275

METHOD

This research employs a normative juridical approach, which focuses on examining legal norms and principles as stipulated in statutory regulations and relevant legal literature.[22] The study relies primarily on secondary data obtained through a comprehensive literature review, including analysis of laws and regulations, scholarly articles, books, and official documents related to cybercrime in Indonesia and Singapore.[23]

Data collection was conducted through library research, sourcing materials from previous research findings, works of legal experts, official government publications, and international legal instruments.[24] The selection of literature was based on its relevance and authority in the field of cyber law, particularly those addressing the Electronic Information and Transactions Law in Indonesia and the Computer Misuse Act and Cybersecurity Act in Singapore.[25]

The data analysis technique used in this research is qualitative and descriptive-analytical.[26] The analysis involves systematically reviewing and comparing the legislative provisions, regulatory frameworks, and law enforcement mechanisms concerning cybercrime in both countries. Special attention is given to the scope of regulated cybercrimes, procedures for handling digital evidence, personal data protection, and international cooperation mechanisms.[27]

Through this normative juridical and comparative approach, the research aims to identify similarities and differences in the legal frameworks of Indonesia and Singapore, as well as to evaluate the effectiveness and challenges in the implementation of cybercrime laws in both jurisdictions.[28]

RESULTS AND DISCUSSION

A. The Evolution and Scope of Cyber Law

Cyber law, or *hukum siber*, is a specialized legal domain that governs all aspects related to the use of the Internet and electronic technology by individuals, organizations, and legal entities.[29] Its scope is remarkably broad, encompassing not only the moment a person or

[22] Johny. Efendi, Jonaedi. Ibrahim, *Metode Penelitian Hukum Normatif Dan Empiris*, 1st ed. (Depok: Prenamedia Group, 2018).
[23] Zainuddin Ali, *Metode Penelitian Hukum*, 1st ed. (Jakarta: Sinar Grafika, 2009).
[24] Singapore Parliament, "The Statutes of The Republic of Singapore Computer Misuse Act 1993," no. December 2021 (1993).
[25] Ramadhan, "Building Cybersecurity Regulation in Southeast Asia: A Challenge for the Association of Southeast Asian Nations (ASEAN)."
[26] Muhammad Ikhya Apriansyah, Maria Maya Lestari, and Evi Deliana, "Efektivitas Asean Treaty On Mutual Legal Assistance (Amlat) Dalam Menghadapi Kejahatan Transnasional Di Negara Indonesia" 5, no. 1 (2024): 50–61.
[27] Oecd, "Cybersecurity Policy Making at a Turning Point. Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy."
[28] Munabari et al., "Cyber Espionage in Indonesia : Legal Challenges and The Role of Institutions in the Digital Era."
[29] Putra, "Kebijakan Aplikasi Tindak Pidana Siber (Cyber Crime) Di Indonesia."

Journal Widya Gama Law Review
Faculty of Law, Universitas Widya Gama Malang
Vol 2, No 1 (2025): April, Page 67-84
e-ISSN: 3063-8275

institution connects to the Internet and enters the virtual world but also the entire spectrum of digital interactions, transactions, and communications that occur in cyberspace.[30] This field of law has become increasingly relevant and indispensable, particularly in countries with advanced digital infrastructure where the integration of technology into daily life is profound and pervasive.[31]

The evolution of cyber law has been driven by the rapid and continuous development of information and communication technology.[32] Innovations such as cloud computing, big data analytics, artificial intelligence, and the Internet of Things (IoT) have revolutionized how people interact, conduct business, and access information. These advancements have created countless opportunities for economic growth, efficiency, innovation, and social connectivity.[33] However, they have also introduced new vulnerabilities and risks, giving rise to a variety of cybercrimes that were previously unimaginable in the pre-digital era.[34]

Cybercrime is inherently transnational; perpetrators can operate from one country and inflict harm in another, exploiting the borderless and decentralized structure of cyberspace.[35] As emphasized, cybercrime transcends traditional boundaries of time and space, making it a global issue that challenges conventional legal frameworks and enforcement mechanisms. The diversity of cybercrime is vast, encompassing offenses such as hacking, data theft, online fraud, the spread of malware and ransomware, cyberbullying, online harassment, defamation, identity theft, intellectual property violations, and the distribution of illegal or harmful content. These crimes can have far-reaching impacts, not only on individual victims but also on businesses, governments, and the broader society.[36]

The borderless nature of cyberspace means that legal issues arising from cyber activities often involve multiple jurisdictions, making investigation, prosecution, and enforcement particularly complex.[37] For instance, a single cyberattack may involve perpetrators, victims, servers, and financial transactions located in different countries, each governed by its own set of laws and regulations.[38] This complexity necessitates the harmonization of legal frameworks and the establishment of effective mechanisms for international cooperation and mutual legal

[30] Rasyikah Md Khalid and Ainul Jaria Maidin, *Good Governance and the Sustainable Development Goals in Southeast Asia*, *Good Governance and the Sustainable Development Goals in Southeast Asia*, 2022, https://doi.org/10.4324/9781003230724.
[31] Robert Brian Smith, "Complexity of Legal Harmonisation in Southeast Asia: A Diversity of Legal Systems & Languages," *Athens Journal of Law* 10, no. 2 (2024): 233–54, https://doi.org/10.30958/ajl.10-2-4.
[32] Khalid and Maidin, *Good Gov. Sustain. Dev. Goals Southeast Asia*.
[33] Rizal and Yani, "Cybersecurity Policy and Its Implementation in Indonesia."
[34] Anonymous, "Cybersecurity Policy Making at a Turning Point."
[35] Thailand, "Treaty on Mutual Legal Assistance in Criminal Matters."
[36] Thailand.
[37] Ioannidis, "Personal Data Protection."
[38] Munabari et al., "Cyber Espionage in Indonesia : Legal Challenges and The Role of Institutions in the Digital Era."

Journal Widya Gama Law Review
Faculty of Law, Universitas Widya Gama Malang
Vol 2, No 1 (2025): April, Page 67-84
e-ISSN: 3063-8275

assistance.[39]

Furthermore, the evolution of cyber law reflects the need to balance various competing interests, such as the protection of privacy and personal data, the promotion of innovation and economic development, the safeguarding of national security, and the upholding of fundamental rights such as freedom of expression.[40] Legislators and policymakers are continually challenged to create laws that are sufficiently flexible to adapt to rapid technological changes, yet robust enough to provide legal certainty and protection for all stakeholders.[41]

In response to these challenges, many countries, including Indonesia and Singapore, have enacted comprehensive cyber laws and regulations.[42] These legal instruments are designed to address the multifaceted nature of cybercrime, regulate electronic transactions, protect personal data, and establish clear procedures for investigating and prosecuting cyber offenses.[43] In Indonesia, for example, the Electronic Information and Transactions Law serves as the primary legal framework for governing digital activities, while Singapore has implemented the Computer Misuse Act and the Cybersecurity Act to safeguard its digital infrastructure and critical information systems.[44]

The ongoing evolution of cyber law also underscores the importance of public awareness and education.[45] As technology becomes increasingly embedded in everyday life, individuals and organizations need to understand their rights and obligations in cyberspace, recognize potential risks, and adopt responsible digital behaviors.[46] Legal frameworks alone are insufficient without the active participation of all stakeholders in fostering a secure, ethical, and resilient digital environment.[47]

In conclusion, the evolution and scope of cyber law are dynamic and expansive, shaped by technological advancements, emerging threats, and the growing interdependence of the global digital ecosystem.[48] As cyber risks continue to evolve, so too must the legal responses,

[39] Obet, Suharto, and Mujoko, "Cyber Cooperation in the Framework of the Asean Regime."
[40] Riko Nugraha, "Perspektif Hukum Indonesia (Cyberlaw) Penanganan Kasus Cyber Di Indonesia," *Jurnal Ilmiah Hukum Dirgantara* 11, no. 2 (2021): 44–56.
[41] Ioannidis, "Personal Data Protection."
[42] Nurfaika Ishak, "Guarantee of Information and Communication Technology Application Security in Indonesia: Regulations and Challenges?," *Audito Comparative Law Journal (ACLJ)* 4, no. 2 (2023): 108–17, https://doi.org/10.22219/aclj.v4i2.26098.
[43] Kandy, Fathoni, and Lubis, "Evolution and Challenges of Cyber Law in the Digital Era : Case Studies in Developing Countries."
[44] Rizal and Yani, "Cybersecurity Policy and Its Implementation in Indonesia."
[45] Kandy, Fathoni, and Lubis, "Evolution and Challenges of Cyber Law in the Digital Era : Case Studies in Developing Countries."
[46] Brenner, "Cybercrime: Criminal Threats from Cyberspace."
[47] Obet, Suharto, and Mujoko, "Cyber Cooperation in the Framework of the Asean Regime."
[48] Cybersecurity Act 2018, "REPUBLIC OF SINGAPORE GOVERNMENT GAZETTE ACTS SUPPLEMENT (Cybersecurity Act No.9 2018)," no. 9 (2018): 72.

Journal Widya Gama Law Review
Faculty of Law, Universitas Widya Gama Malang
Vol 2, No 1 (2025): April, Page 67-84
e-ISSN: 3063-8275

requiring ongoing adaptation, collaboration, and innovation at both the national and international levels.[49]

B. Cyber Law Enforcement in Indonesia

In Indonesia, the significance of cyber law is reflected in the enactment of Law Number 11 of 2008 concerning Electronic Information and Transactions, which was subsequently amended by Law Number 19 of 2016.[50] This legislation serves as the principal legal umbrella for regulating a wide range of activities involving information technology, electronic transactions, and digital communication.[51] The Electronic Information and Transactions Law aims to provide legal certainty, protect the rights and interests of users, and ensure the safe, responsible, and ethical use of digital platforms within Indonesia's jurisdiction.[52]

The Electronic Information and Transactions Law is comprehensive in its coverage, addressing various aspects such as the validity of electronic documents and signatures, the regulation of electronic contracts, the prevention and prosecution of cybercrimes, and the protection of personal data.[53] It also establishes criminal provisions for offenses such as unauthorized access, electronic fraud, online defamation, the dissemination of illegal content, and violations of privacy.[54] By doing so, the Electronic Information and Transactions Law seeks to create a secure digital environment that fosters trust and confidence among users, businesses, and government institutions.[55]

Despite its broad scope and ambitious objectives, the implementation of the Electronic Information and Transactions Law in Indonesia continues to face significant challenges.[56] Law enforcement against cybercrime is often hampered by limited resources, including insufficient funding, inadequate technological infrastructure, and a lack of advanced forensic tools necessary for investigating complex digital offenses.[57] The rapid evolution of technology frequently outpaces the capacity of law enforcement agencies, making it difficult to keep up

[49] Apriansyah, Lestari, and Deliana, "Efektivitas Asean Treaty On Mutual Legal Assistance (Amlat) Dalam Menghadapi Kejahatan Transnasional Di Negara Indonesia."
[50] Republik, UU ITE Nomor 19 Tahun 2016.
[51] Suhendi and Asmadi, "Cyber Laws Related to Prevention of Theft of Information Related to Acquisition of Land and Infrastructure Resources in Indonesia."
[52] Saefullah, *Jurisdiksi Sebagai Upaya Penegakan Hukum Cyber Space* (Pusat Studi Cyber Law Fakultas Hukum UNPAD, 2009).
[53] Ioannidis, "Personal Data Protection."
[54] "United Nations Office on Drugs and Crime (UNODC)," n.d., https://www.unodc.org/unodc/en/cybercrime/home.html.
[55] Suhendi and Asmadi, "Cyber Laws Related to Prevention of Theft of Information Related to Acquisition of Land and Infrastructure Resources in Indonesia."
[56] Munabari et al., "Cyber Espionage in Indonesia : Legal Challenges and The Role of Institutions in the Digital Era."
[57] Ioannidis, "Personal Data Protection."

Journal Widya Gama Law Review
Faculty of Law, Universitas Widya Gama Malang
Vol 2, No 1 (2025): April, Page 67-84
e-ISSN: 3063-8275

with new methods and tactics employed by cybercriminals.[58]

Another major challenge is the shortage of specialized expertise among law enforcement personnel, prosecutors, and judges.[59] Many legal practitioners and investigators have not received adequate training in digital forensics, cyber investigation techniques, or the interpretation of electronic evidence, which can undermine the effectiveness of criminal prosecutions.[60] The lack of inter-agency coordination and the absence of dedicated cybercrime units in some regions further exacerbate these difficulties.[61]

Furthermore, public legal awareness regarding cybercrime remains relatively low in Indonesia.[62] Many individuals and organizations are unaware of their rights and obligations under the Electronic Information and Transactions Law and do not fully understand the risks associated with online activities.[63] This lack of awareness impedes both the prevention and reporting of cybercrimes, as victims may not recognize when their rights have been violated or may be reluctant to engage with law enforcement due to concerns over privacy, stigma, or distrust of authorities.[64] As highlighted by Didik M. Arief Mansur and Elisatris Gultom, the lack of knowledge and understanding about cybercrime among the Indonesian population contributes to weak legal compliance and insufficient community supervision over suspicious online activities.[65]

In addition to these internal challenges, Indonesia also faces external threats due to the transnational nature of cybercrime.[66] Cyberattacks can originate from abroad and target Indonesian individuals, companies, or critical infrastructure, complicating efforts to identify perpetrators and bring them to justice.[67] The need for international cooperation and mutual legal assistance is therefore increasingly urgent, especially as cyber threats become more sophisticated and cross-border in nature.[68]

To address these multifaceted challenges, several strategic measures are necessary. First,

[58] Ishak, "Guarantee of Information and Communication Technology Application Security in Indonesia: Regulations and Challenges?"
[59] Oecd, "Cybersecurity Policy Making at a Turning Point. Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy."
[60] Ioannidis, "Personal Data Protection."
[61] Oecd, "Cybersecurity Policy Making at a Turning Point. Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy."
[62] Makarim. Edmon, *Kompilasi Hukum Telematika* (Jakarta: Raja Grafindo Persada, 2003).
[63] Nugraha, "Perspektif Hukum Indonesia (Cyberlaw) Penanganan Kasus Cyber Di Indonesia."
[64] Asosiasi Profesional Privasi Data Indonesia, "Data Protection Law in Singapore – Privacy and Sovereignty in an Interconnected World," n.d., https://appdi.org/data-protection-law-in-singapore-privacy-and-sovereignty-in-an-interconnected-world/.
[65] Putra, "Kebijakan Aplikasi Tindak Pidana Siber (Cyber Crime) Di Indonesia."
[66] Eliasta Ketaren, "Cybercrime, Cyber Space, Dan Cyber Law," *Jurnal TIMES* 5, no. 2 (2017): 35–42, https://doi.org/10.51351/jtm.5.2.2016556.
[67] Thailand, "Treaty on Mutual Legal Assistance in Criminal Matters."
[68] Brenner, "Cybercrime: Criminal Threats from Cyberspace."

e-ISSN: 3063-8275

public legal education must be enhanced through awareness campaigns, school curricula, and community outreach programs to promote responsible digital behavior and a better understanding of cyber law.[69] Second, the capacity of law enforcement agencies should be strengthened by providing specialized training, modern investigative tools, and establishing dedicated cybercrime units at both the national and regional levels.[70] Third, Indonesia needs to develop more specific and detailed regulations (lex specialis) that can address the rapidly evolving nature of cyber threats, such as sector-specific cybersecurity standards and a comprehensive personal data protection law.[71]

Moreover, continuous legal reform and adaptation are essential to ensure that the Electronic Information and Transactions Law remains relevant and effective in the face of technological advancements.[72] This includes regularly updating legal definitions, procedures for handling electronic evidence, and sanctions for emerging types of cyber offenses.[73] Collaboration with international partners, participation in regional initiatives such as those led by ASEAN, and active engagement in global forums on cybersecurity are also vital to improving Indonesia's resilience against cyber threats.[74]

In summary, while Indonesia has made significant progress in establishing a legal framework for cyber law enforcement, ongoing efforts are required to overcome practical challenges in implementation.[75] By enhancing public awareness, building institutional capacity, refining legal provisions, and fostering international cooperation, Indonesia can strengthen its ability to protect its digital ecosystem and uphold justice in cyberspace.[76]

C. Cyber Law and Enforcement in Singapore

Singapore, by contrast, has established a more integrated and systematic approach to managing cybersecurity.[77] The country is recognized for its robust legal and institutional framework, which is reflected in several key pieces of legislation.[78] The Cybersecurity Act 2018 is a cornerstone of Singapore's cyber law regime, providing a comprehensive framework

[69] Access Partnership, "Norms For Cybersecurity in Southeast Asia: Policy Options for Collaborative Security in the Southeast Asian Region."
[70] Ramadhan, "Building Cybersecurity Regulation in Southeast Asia: A Challenge for the Association of Southeast Asian Nations (ASEAN)."
[71] Choo, "The Cyber Threat Landscape: Challenges and Future Research Directions."
[72] Nugraha, "Perspektif Hukum Indonesia (Cyberlaw) Penanganan Kasus Cyber Di Indonesia."
[73] Association of Southeast Asian Nations, "ASEAN Cybersecurity Cooperation Strategy (2021-2025)."
[74] Ramadhan, "Building Cybersecurity Regulation in Southeast Asia: A Challenge for the Association of Southeast Asian Nations (ASEAN)."
[75] Brenner, "Cybercrime: Criminal Threats from Cyberspace."
[76] Nurse et al., "Cybersecurity Awareness. In: Encyclopedia of Cryptography, Security and Privacy."
[77] Interpol, "CONNECTING POLICE FOR A SAFER WORLD 2020 Contents," 2020, www.interpol.int.
[78] Nugraha, "Perspektif Hukum Indonesia (Cyberlaw) Penanganan Kasus Cyber Di Indonesia."

for managing cyber threats and protecting critical information infrastructure. The Act mandates the identification and protection of critical sectors, incident reporting, and empowers the Cyber Security Agency (CSA) to coordinate national cybersecurity efforts.[79]

In addition to the Cybersecurity Act, Singapore enacted the Personal Data Protection Act 2012 (PDPA), which regulates the collection, use, and disclosure of personal data by organizations.[80] The PDPA is closely aligned with international standards such as the European Union's General Data Protection Regulation (GDPR), ensuring that Singapore's data protection regime is both rigorous and globally compatible.[81]

Singapore's approach extends beyond domestic regulation; the country actively participates in international cooperation to combat cybercrime.[82] This includes bilateral and multilateral agreements for information sharing, joint investigations, and the extradition of cybercriminals.[83] Singapore's proactive stance has positioned it as a regional leader in cybersecurity and data protection.[84]

D. Comparative Analysis: Legal Provisions and Enforcement

Definition and Scope

1. **Singapore:**[85]

   The Computer Misuse Act 1993 targets unauthorized access, the spread of malicious software, and other computer-related offenses. The Cybersecurity Act 2018 focuses on the protection of critical information infrastructure and mandates strict reporting and response protocols for cyber incidents.

2. **Indonesia:**[86]

   The Electronic Information and Transactions Law defines various terms related to electronic information, transactions, and documents. Its scope includes electronic fraud, illegal content dissemination, defamation, privacy violations, and other offenses committed via digital means.

[79] Cybersecurity Act 2018, "REPUBLIC OF SINGAPORE GOVERNMENT GAZETTE ACTS SUPPLEMENT (Cybersecurity Act No.9 2018)."
[80] Nurse et al., "Cybersecurity Awareness. In: Encyclopedia of Cryptography, Security and Privacy."
[81] Asosiasi Profesional Privasi Data Indonesia, "Data Protection Law in Singapore – Privacy and Sovereignty in an Interconnected World."
[82] Caroline Kuzemko, "The Importance of Transformative Politics," n.d.
[83] Singapore Parliament, "The Statutes of The Republic of Singapore Computer Misuse Act 1993."
[84] Smith, "Complexity of Legal Harmonisation in Southeast Asia: A Diversity of Legal Systems & Languages."
[85] Singapore Parliament, "The Statutes of The Republic of Singapore Computer Misuse Act 1993."
[86] Putra, "Kebijakan Aplikasi Tindak Pidana Siber (Cyber Crime) Di Indonesia."

Journal Widya Gama Law Review
Faculty of Law, Universitas Widya Gama Malang
Vol 2, No 1 (2025): April, Page 67-84
e-ISSN: 3063-8275

Subjects and Objects

1. **Singapore:**[87]

   The primary subjects are critical information infrastructure operators, while the objects of protection are systems and data vital to national security and public welfare.

2. **Indonesia:**[88]

   Subjects include individuals and legal entities operating electronic systems, while objects encompass electronic information, electronic documents, and the integrity of digital transactions.

Legal Basis and Jurisdiction

1. **Singapore:**[89]

   The Cybersecurity Act 2018 and the Computer Misuse Act 1993 form the backbone of cyber law, with the Cyber Security Agency (CSA) as the main authority.

2. **Indonesia:**[90]

   The Electronic Information and Transactions Law No. 19 of 2016 is enforced by the Ministry of Communication and Information, with investigative and prosecutorial functions carried out by the police and prosecutors.

Specification of Criminal Offenses

1. **Singapore:**[91]

   Offenses include unauthorized access, interference with critical information infrastructure, and failure to report cyber incidents. The law emphasizes prevention and rapid response to threats.

2. **Indonesia:**[92]

   The Electronic Information and Transactions Law covers a wider array of offenses, including the dissemination of illegal content, online defamation, cyber fraud, and privacy violations. However, its general nature sometimes leads to interpretative ambiguities.

[87] The Law Revision Commission, "The Statutes of The Republic of Singapore Personal Data Protection Act 2012," no. December 2021 (2020): 124, https://sso.agc.gov.sg/Act/PDPA2012?ViewType=Pdf&_=20210111164941.
[88] Republik, UU ITE Nomor 19 Tahun 2016.
[89] Ramadhan, "Building Cybersecurity Regulation in Southeast Asia: A Challenge for the Association of Southeast Asian Nations (ASEAN)."
[90] Munabari et al., "Cyber Espionage in Indonesia : Legal Challenges and The Role of Institutions in the Digital Era."
[91] Cybersecurity Act 2018, "REPUBLIC OF SINGAPORE GOVERNMENT GAZETTE ACTS SUPPLEMENT (Cybersecurity Act No.9 2018)."
[92] Kandy, Fathoni, and Lubis, "Evolution and Challenges of Cyber Law in the Digital Era : Case Studies in Developing Countries."

Journal Widya Gama Law Review
Faculty of Law, Universitas Widya Gama Malang
Vol 2, No 1 (2025): April, Page 67-84
e-ISSN: 3063-8275

Personal Data Protection

1. **Singapore:**[93]

   The PDPA provides a comprehensive legal framework for the protection of personal data, imposing strict obligations on organizations and granting enforceable rights to individuals.

2. **Indonesia:**[94]

   While the Electronic Information and Transactions Law addresses certain aspects of data protection, a dedicated and comprehensive personal data protection law is still under development, highlighting a gap in Indonesia's legal framework.

Table 1.

Comparison of Indonesia and Singapore

Source: author, 2024.

Aspects	Indonesia (UU ITE No.19/2016)	Singapura (Computer Misuse Act & Cybersecurity Act)
Definition Cybercrime	Broad, covering illegal content, fraud, etc.	Focus on illegal access, sabotage, and critical infrastructure protection.
Personal Data Protection	There is no specific law yet	PDPA 2012 provides strong personal data protection
Law Enforcement	Ministry of Communication and Information and the Police	Cyber Security Agency and Police
International Cooperation	ASEAN extradition and MLA treaties	Active in bilateral and multilateral cooperation

E. International Cooperation and Regional Initiatives

Given the transnational nature of cybercrime, international cooperation is indispensable. Both Indonesia and Singapore are parties to various treaties and agreements that facilitate cross-border law enforcement.[95]

[93] The Law Revision Commission, "The Statutes of The Republic of Singapore Personal Data Protection Act 2012."
[94] Ishak, "Guarantee of Information and Communication Technology Application Security in Indonesia: Regulations and Challenges?"
[95] Association of Southeast Asian Nations, "ASEAN Cybersecurity Cooperation Strategy (2021-2025)."

Journal Widya Gama Law Review
Faculty of Law, Universitas Widya Gama Malang
Vol 2, No 1 (2025): April, Page 67-84
e-ISSN: 3063-8275

1. **Extradition Treaties:**[96]

   The 2019 Extradition Treaty between Indonesia and Singapore includes provisions for cybercrime, enabling the transfer of suspects and convicts to ensure accountability.

2. **Mutual Legal Assistance (MLA):**[97]

   The ASEAN Mutual Legal Assistance Treaty (AMLAT) provides a platform for regional cooperation in the investigation and prosecution of cybercrime, facilitating the exchange of evidence and information.

3. **Law Enforcement Cooperation:**[98]

   Joint cyber patrols, joint investigation teams, and capacity-building initiatives are regularly conducted to enhance the effectiveness of cyber law enforcement in the region.

4. **ASEAN's Role:**[99]

   ASEAN has developed various initiatives to strengthen the regional cyber legal framework, enhance law enforcement capacity, promote intelligence sharing, and foster public-private partnerships.

F. Basic Principles of International Cyber Law

International cyber law is guided by several foundational principles aimed at ensuring security, stability, and justice in cyberspace:[100]

1. **State Sovereignty:**[101]

   Each country has the right to regulate its cyberspace, but must respect human rights and refrain from interfering in the affairs of other nations.

2. **International Cooperation:**[102]

   Countries should collaborate to combat cybercrime, protect human rights online, and promote responsible use of technology through treaties and international organizations.

[96] Anonymous, "Cybersecurity Policy Making at a Turning Point."
[97] "Computer Crime Act Di Singapura," n.d., https://www.cybercrimelaw.net/Singapore.html.
[98] Kshetri, *Cybercrime and Cybersecurity in the Global South*.
[99] James Tan et al., "ASEAN Cyberthreat Assessment 2021," *Interpol*, 2021, 5, https://www.interpol.int/content/download/16106/file/ASEAN Cyberthreat Assessment 2021 - final.pdf.
[100] Smith, "Complexity of Legal Harmonisation in Southeast Asia: A Diversity of Legal Systems & Languages."
[101] Rizal and Yani, "Cybersecurity Policy and Its Implementation in Indonesia."
[102] Ishak, "Guarantee of Information and Communication Technology Application Security in Indonesia: Regulations and Challenges?"

e-ISSN: 3063-8275

3. **Freedom of Expression:**[103]

   While freedom of expression is fundamental, it must be balanced against the need to prevent hate speech, misinformation, and illegal content.

4. **Data Privacy:**[104]

   Individuals have the right to control their personal information, and states must enact laws to protect data privacy and promote responsible data processing.

5. **Cybersecurity:**[105]

   Governments, the private sector, and civil society share responsibility for securing digital infrastructure and raising public awareness.

6. **Equal Access:**[106]

   Efforts must be made to ensure all individuals have equitable access to information and communication technology, bridging the digital divide.

7. **Accountability:**[107]

   All actors in cyberspace must be held accountable for their actions, with effective legal frameworks for investigation and prosecution.

8. **Law Enforcement and Capacity Building:**[108]

   States must invest in effective legislation, trained law enforcement, and continuous education to keep pace with evolving cyber threats.

CONCLUSION

A comparison of the cyber legal systems between Indonesia and Singapore shows that while both have developed significant legal frameworks in the face of cybercrime, the approaches taken differ greatly in terms of regulatory effectiveness and specificity. Singapore features a more integrated and risk-based model, particularly through the implementation of the Cybersecurity Act and Personal Data Protection Act which provide comprehensive protection to critical infrastructure and personal data. On the other hand, Indonesia still relies on a generalistic approach through the ITE Law which, despite its broad scope, still

[103] Tan et al., "ASEAN Cyberthreat Assessment 2021."
[104] OECD, "OECD Policy Framework on Digital Security: Cybersecurity for Prosperity," 2022.
[105] Kandy, Fathoni, and Lubis, "Evolution and Challenges of Cyber Law in the Digital Era : Case Studies in Developing Countries."
[106] Obet, Suharto, and Mujoko, "Cyber Cooperation in the Framework of the Asean Regime."
[107] Michael Hanna, "Exploring Cybersecurity Awareness and Training Strategies To Walden University," 2020.
[108] ASEAN, "Asean Cyberthreat Assessment 2020 Key Insights From the Asean Cybercrime Operations Desk," 2020, https://asean.org/wp-content/uploads/2021/01/ASEAN_CyberThreatAssessment_2020.pdf.

experiences obstacles in terms of norm clarity, law enforcement, and personal data protection which does not yet have its own legal basis.

The main weaknesses faced by Indonesia include the lack of technical capacity of law enforcement officers, weak inter-agency coordination, and low public awareness of cyber law. This situation exacerbates vulnerability to transnational cyberattacks and complicates law enforcement efforts. As an implication of these findings, there are several strategic steps that need to be taken:

1. Drafting and passing a comprehensive Personal Data Protection Law that is in line with international standards.
2. Capacity building of law enforcement agencies, including digital forensics training and the establishment of specialized cyber units at the national and regional levels.
3. Harmonization of regional cyber laws through strengthening ASEAN's role in establishing harmonized legal frameworks and operational cooperation mechanisms.
4. Expansion of cyber law education to the public, especially the younger generation, to improve digital literacy and resilience to cyber risks.

By adopting a strategic and collaborative approach like Singapore's, Indonesia can strengthen its legal resilience against cybercrime and improve digital justice and security for all citizens. This research is expected to serve as a normative and comparative basis for policy makers in formulating cyber policies that are more effective, responsive and adaptive in the digital era.

REFERENCES

Access Partnership. "Norms For Cybersecurity in Southeast Asia: Policy Options for Collaborative Security in the Southeast Asian Region," 2017, 20. https://ccapac.asia/wp-content/uploads/2022/03/Norms-for-Cybersecurity-in-Southeast-Asia.pdf.

Ali, Zainuddin. *Metode Penelitian Hukum*. 1st ed. Jakarta: Sinar Grafika, 2009.

Anonymous. "Cybersecurity Policy Making at a Turning Point." *OECD Digital Economy Papers*, no. 211 (2012): 0_1,2,4-56. http://search.proquest.com.library.capella.edu/docview/1223514107?accountid=27965%5Cnhttp://wv9lq5ld3p.search.serialssolutions.com.library.capella.edu/?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/ABI/INFORM+Global&rft_val_fmt=info:ofi/f.

Apriansyah, Muhammad Ikhya, Maria Maya Lestari, and Evi Deliana. "Efektivitas Asean Treaty On Mutual Legal Assistance (Amlat) Dalam Menghadapi Kejahatan Transnasional Di

Negara Indonesia" 5, no. 1 (2024): 50–61.

ASEAN. "Asean Cyberthreat Assessment 2020 Key Insights From the Asean Cybercrime Operations Desk," 2020. https://asean.org/wp-content/uploads/2021/01/ASEAN_CyberThreatAssessment_2020.pdf.

ASEAN Secretariat. "Badan Siber Dan Sandi Negara (BSSN)," n.d.

Asosiasi Profesional Privasi Data Indonesia. "Data Protection Law in Singapore – Privacy and Sovereignty in an Interconnected World," n.d. https://appdi.org/data-protection-law-in-singapore-privacy-and-sovereignty-in-an-interconnected-world/.

Association of Southeast Asian Nations. "ASEAN Cybersecurity Cooperation Strategy (2021-2025)." *Asean.Org*, 2022, 1–14. https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf.

Brenner, Susan W. "Cybercrime: Criminal Threats from Cyberspace." *Cybercrime: Criminal Threats from Cyberspace*, 2010, 1–283. https://doi.org/10.5860/choice.48-0685.

Choo, Kim Kwang Raymond. "The Cyber Threat Landscape: Challenges and Future Research Directions." *Computers and Security* 30, no. 8 (2011): 719–31. https://doi.org/10.1016/j.cose.2011.08.004.

"Computer Crime Act Di Singapura," n.d. https://www.cybercrimelaw.net/Singapore.html.

"Council of Europe Convention on Cybercrime," n.d. https://www.coe.int/en/web/cybercrime/the-%0Abudapest-convention%0A.

Cybersecurity Act 2018. "REPUBLIC OF SINGAPORE GOVERNMENT GAZETTE ACTS SUPPLEMENT (Cybersecurity Act No.9 2018)," no. 9 (2018): 72.

Edmon, Makarim. *Kompilasi Hukum Telematika*. Jakarta: Raja Grafindo Persada, 2003.

Efendi, Jonaedi. Ibrahim, Johny. *Metode Penelitian Hukum Normatif Dan Empiris*. 1st ed. Depok: Prenamedia Group, 2018.

Hanna, Michael. "Exploring Cybersecurity Awareness and Training Strategies To Walden University," 2020.

Interpol. "CONNECTING POLICE FOR A SAFER WORLD 2020 Contents," 2020. www.interpol.int.

Ioannidis, Nikolas. "Personal Data Protection." *Border Control and New Technologies*, 2021, 61–80. https://doi.org/10.46944/9789461171375.4.

Ishak, Nurfaika. "Guarantee of Information and Communication Technology Application Security in Indonesia: Regulations and Challenges?" *Audito Comparative Law Journal (ACLJ)* 4, no. 2 (2023): 108–17. https://doi.org/10.22219/aclj.v4i2.26098.

Kandy, Samra Al, Tamrin Fathoni, and Arief Fahmi Lubis. "Evolution and Challenges of Cyber

Law in the Digital Era : Case Studies in Developing Countries" 1, no. 1 (2024): 1–10.

Ketaren, Eliasta. "Cybercrime, Cyber Space, Dan Cyber Law." *Jurnal TIMES* 5, no. 2 (2017): 35–42. https://doi.org/10.51351/jtm.5.2.2016556.

Khalid, Rasyikah Md, and Ainul Jaria Maidin. *Good Governance and the Sustainable Development Goals in Southeast Asia*. *Good Governance and the Sustainable Development Goals in Southeast Asia*, 2022. https://doi.org/10.4324/9781003230724.

Kshetri, Nir. *Cybercrime and Cybersecurity in the Global South*. GOVERNING GLOBAL PRODUCTION, 2013.

Kuzemko, Caroline. "The Importance of Transformative Politics," n.d.

Munabari, Fahlesa, Eko Daryanto, Stanislaus Riyanta, and Margaretha Hanita. "Cyber Espionage in Indonesia : Legal Challenges and The Role of Institutions in the Digital Era" 8 (2024): 109–31.

Nugraha, Riko. "Perspektif Hukum Indonesia (Cyberlaw) Penanganan Kasus Cyber Di Indonesia." *Jurnal Ilmiah Hukum Dirgantara* 11, no. 2 (2021): 44–56.

Nurse, Jason R. C., S. Jajodia, P. Samarati, and M. Yung. "Cybersecurity Awareness. In: Encyclopedia of Cryptography, Security and Privacy." *Kent University Repository*, 2021, 1–4.

Obet, Dedy, Suharto Suharto, and Henri Mujoko. "Cyber Cooperation in the Framework of the Asean Regime." *Jurnal Pertahanan: Media Informasi Ttg Kajian & Strategi Pertahanan Yang Mengedepankan Identity, Nasionalism & Integrity* 7, no. 2 (2021): 254. https://doi.org/10.33172/jp.v7i2.1264.

Oecd. "Cybersecurity Policy Making at a Turning Point. Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy." *Organisation for Economic Co-Operation and Development*, 2012. https://doi.org/http://dx.doi.org/10.1787/5k8zq92vdgtl-en.

OECD. "OECD Policy Framework on Digital Security: Cybersecurity for Prosperity," 2022.

Putra, Budi Kristian Bivanda. "Kebijakan Aplikasi Tindak Pidana Siber (Cyber Crime) Di Indonesia." *Pamulang Law Review* 1, no. 1 (2019): 1. https://doi.org/10.32493/palrev.v1i1.2842.

Ramadhan, Iqbal. "Building Cybersecurity Regulation in Southeast Asia: A Challenge for the Association of Southeast Asian Nations (ASEAN)." *Journal of Social and Political Sciences* 3, no. 4 (2020). https://doi.org/10.31014/aior.1991.03.04.230.

Republik, Indonesia. UU ITE Nomor 19 Tahun 2016, Pub. L. No. 19, 44 Journal of Physics A: Mathematical and Theoretical 287 (2016). file:///C:/Users/Lenovo/Downloads/UU Nomor

e-ISSN: 3063-8275

19 Tahun 2016.pdf.

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

Saefullah. *Jurisdiksi Sebagai Upaya Penegakan Hukum Cyber Space*. Pusat Studi Cyber Law Fakultas Hukum UNPAD, 2009.

Singapore Parliament. "The Statutes of The Republic of Singapore Computer Misuse Act 1993," no. December 2021 (1993).

Smith, Robert Brian. "Complexity of Legal Harmonisation in Southeast Asia: A Diversity of Legal Systems & Languages." *Athens Journal of Law* 10, no. 2 (2024): 233–54. https://doi.org/10.30958/ajl.10-2-4.

Suhendi, Dadang, and Erwin Asmadi. "Cyber Laws Related to Prevention of Theft of Information Related to Acquisition of Land and Infrastructure Resources in Indonesia." *International Journal of Cyber Criminology* 15, no. 2 (2021): 135–43. https://doi.org/10.5281/zenodo.4766552.

Tan, James, Wei Xian Tee, Adam Parsons, and Alyssa Radlett. "ASEAN Cyberthreat Assessment 2021." *Interpol*, 2021, 5. https://www.interpol.int/content/download/16106/file/ASEAN Cyberthreat Assessment 2021 - final.pdf.

Thailand, the Union of Myanmar and the Kingdom of. "Treaty on Mutual Legal Assistance in Criminal Matters." *Sustainability (Switzerland)*, 2006. http://scioteca.caf.com/bitstream/handle/123456789/1091/RED2017-Eng-8ene.pdf?sequence=12&isAllowed=y%0Ahttp://dx.doi.org/10.1016/j.regsciurbeco.2008.06.005%0Ahttps://www.researchgate.net/publication/305320484_SISTEM_PEMBETUNGAN_TERPUSAT_STRATEGI_MELESTARI.

The Law Revision Commission. "The Statutes of The Republic of Singapore Personal Data Protection Act 2012," no. December 2021 (2020): 124. https://sso.agc.gov.sg/Act/PDPA2012?ViewType=Pdf&_=20210111164941.

"United Nations Office on Drugs and Crime (UNODC)," n.d. https://www.unodc.org/unodc/en/cybercrime/home.html.