PROPHETIC LAW REVIEW
Volume 5, Issue 1, June 2023

BETWEEN FREEDOM AND PROTECTION: A CRITICAL REVIEW OF INDONESIA'S CYBERSPACE LAW

Haekal Al Asyari[1]

Citation Guide:
Haekal Al Asyari, '**BETWEEN FREEDOM AND PROTECTION: A CRITICAL REVIEW OF INDONESIA'S CYBERSPACE LAW**' [2023] 5 (1) Prophetic Law Review 79.

Received:
29 Maret 2023
Accepted:
10 June 2023
Published:
4 July 2023

DOI:
10.20885/PLR.vol5.iss1.art5

Abstract

Following the COVID-19 pandemic, dependency on the internet—notably, the utilization of cyberspace—has increased, amplifying the virtual domain to a prominent role in everyone's everyday life. As a country with one of the highest number of internet users in Asia, Indonesia faces challenges of unequal access, limits on content, data privacy, data security, and digital literacy. Given that cyberspace infrastructure is shared between governments, corporations, individuals, and telecommunication providers while individual countries govern the networks, the Indonesian government is under its own exclusive authority to legislate and create policies governing Indonesia's cyberspace. There has been significant progress toward a legal framework of Indonesia's cyberspace law, such as the enactment of the Personal Data Protection Law. Unfortunately, such progress is far from being effective. It is evident from Indonesia's fragmented laws, response-driven policies, and the numerous cyber incidents that have occurred only within the past years. This article investigates Indonesia's legal-philosophical position in governing the cyberspace. By using a normative methodology, this research crystallizes Indonesia's position between the freedom or the protectionist approach through analyzing the existing cyberspace regulations. The result of this study shows that Indonesia is somewhere in the middle of liberalizing its cyberspace and protecting it for its national interest. This position could bring both advantages and disadvantages to Indonesia's cyberspace development.

Keywords: *Cyberspace, Freedom, Indonesia, Protection.*

[1] Doctoral candidate, Marton Géza Doctoral School of Legal Studies (University of Debrecen, Hungary) and Lecturer of International Law, Faculty of Law, Universitas Gadjah Mada. E-mail: haekal.al.asyari@ugm.ac.id.

A. Introduction

The development of technology and human-digital interactions has opened numerous avenues of opportunity for society and has exposed the weaknesses in technology legislation.[2] The increasing number of cyber threats against the public and private sector provides urgency to improve privacy and security protections in cyberspace. In doing so, a comprehensive legal framework with a philosophical basis suited to Indonesia's ideology is required. Governing cyberspace has been attempted since the internet was founded.[3] There have been various approaches to regulating the internet, and Indonesia's approach is considered unique.

As one of the centerpieces of e-commerce activity in Southeast Asia and with one of the highest internet user base in the region, it is no surprise that Indonesia has become one of the hot spots for 'suspicious web activities.'[4] Indonesia has become a preferred target for cyberattacks due to the massive number of internet users possessing massive user data.[5] However, this is not the only reason behind these attacks. Indonesia's legal framework that governs cyberspace is known to be insufficient and redundant.[6] The laws are often outdated, overcomplicated by bureaucracy, and lack enforcement.[7] Nonetheless, in the past few years, Indonesia has made significant progress towards a more comprehensive legal framework.[8]

Indonesia's primary foundation for governing cyberspace is Law No. 11 of 2008 on Information and Electronic Transactions. It serves as the basis for formulating regulations and policies related to information and security.[9] Recently, the Indonesian Parliament (DPR) passed Law No. 27 of 2022 on Personal Data Protection.[10] Such enactment made

[2] Kriangsak Kittichaisaree. *Public International Law of Cyberspace. Law, Governance and Technology Serie*s (Springer, 2019).

[3] David Post. "Governing Cyberspace: Law" (2018) 24 Santa Clara High Tech. L.J. 883.

[4] Jirapon Sunkpho, Sarawut Ramjan, Chaiwat Oottamakorn. "Cybersecurity Policy in ASEAN Countries" Information Institute Conferences in Las Vegas (2018).

[5] Damien Puyvelde and Aaron Brantly. *Cybersecurity: Politics, Governance and Conflict in Cyberspace* (Polity Press 2019).

[6] . Sarah Safira Aulianisa and Indirwan Indirwan. "Critical Review of the Urgency of Strengthening the Implementation of Cyber Security and Resilience in Indonesia" (2020) 4 Lex Scientia Law Review 30; Noor Halimah Anjani. "Perlindungan Keamanan Siber di Indonesia" Center for Indonesian Policy Studies (2021); Miftahur Rokhman Habibi and Isnatul Liviani. "Kejahatan Teknologi Informasi dan Penanggulangannya dalam Sistem Hukum Indonesia" (2020) 23 Al-Qānūn: Jurnal Pemikiran dan Pembaharuan Hukum Islam 400.

[7] *See* I Nyoman Sukayasa and Wayan Suryathi. "Law Implementation of Cybercrime in Indonesia" (2018) 8 Journal of Social Sciences and Humanities 123; Miftahur Rokhman Habibi and Isnatul Liviani (n 6).

[8] Jirapon Sunkpho, Sarawut Ramjan, Chaiwat Oottamakorn (n 4).

[9] Law No. 11 of 2008 on Electronic Information and Transaction.

[10] Law No. 27 of 2022 on Personal Data Protection.

significant progress towards protecting citizens' data and privacy. Other laws that relate to regulating users' activities on the internet include the Law on Telecommunication, Law on Broadcasting, Law on the Openness of Public Information, Law on State Intelligence, Antipornographic Act, Copyright Act, Consumer Protection Act, Criminal and Procedural Code, Multimedia Convergence Act, National Defense Act, and the Ministerial Regulation concerning Cyber Defense Guideline. With all those laws in place, however, Indonesia has not yet enacted specific laws concerning cyber security. This means that the landscape of Indonesia's cyberspace law is both diverse and incomplete. Despite this, there seems to be a consistent consideration in all those laws of religious and social-cultural values of Indonesian society. This article criticizes such due regard in the context of the two general approaches to cyberspace governance: freedom and protectionism.[11]

Other terms have been coined to describe the two approaches, cyber liberalism and cyber protectionism.[12] The prior opts for complete freedom and unlimited access to cyberspace, while the latter suppresses such freedoms and promotes heavy regulation by the government.[13] Cyber protectionism is a broad term that refers to a wide range of barriers to digital trade (e-commerce) and cross-border data flow,[14] such as censorship, filtering, localization measures, and regulations to protect privacy.[15] Meanwhile, cyber liberalism mainly comprises the right to internet access, freedom of expression and information, as well as freedom from internet censorship. This article found that Indonesia's broad scope and regulations causes inconsistencies to the point that it may strongly support openness for the use internet and may not hesitate to silence or shut down the internet when needed.

Such divergent approaches will determine the reflection of Indonesia's ideological values towards cyberspace governance and the effectiveness of the regulations. Different types of regulation will determine different user behaviors reacting to the limits of their activities in cyberspace.[16] These regulations may take off from a positivist orientation,

[11] This terminology is developed by the author, based on a prior unpublished article titled "Cyberspace ethics: finding an equilibrium between freedom and protectionism" that is under review at the Notre Dame Journal of Law, Ethics, & Public Policy at the time of this writing.

[12] Timothy S. Wu. "Cyberspace Sovereignty? – The Internet and the International System" (1997) 10 Harvard Journal of Law & Technology 648.

[13] Susan Ariel Aaronson. "What Are We Talking about When We Talk about Digital Protectionism?" (2019) 18 World trade review 541.

[14] Susan Ariel Aaronson (n 13).

[15] US Commission. "United States International Trade Commission" (2013).

[16] David R Johnson and David Post. "Law and Borders: The Rise of Law in Cyberspace" (1996) 48 First Monday 1367.

often leaving out the crucial philosophical basis for such norms. Here, a critical analysis is needed to view existing cyberspace law to prevent overlap and ensure effectiveness in regulation.

Several studies have focused on Indonesia's cyberspace law such as cybersecurity,[17] data protection,[18] and cybercrime,[19] but very few have offered a holistic approach to viewing the Indonesian cyberspace legal framework. A critical analysis at such laws is needed to ensure a coherent ideological and/or philosophical stance that is suited to Indonesia. Thus, this article fills in such literary gap.

By employing a normative methodology, this article analyzes the existing legal framework of Indonesia's laws that are specifically aimed at governing cyberspace. These laws include Law No. 11 of 2008 on Information and Electronic Transaction, Law No. 27 of 2022 on Personal Data Protection, and Law No. 44 of 2008 on Antipornography. The selection of such laws is based on the majority scope of cyberspace law that encompasses privacy, data protection, internet content, and cybersecurity.

Thus, this research clarifies Indonesia's cyberspace law ideological/philosophical position between the liberalist and protectionist approaches. The Author hopes that future cyberspace laws will have a firmer philosophical stance suited to Indonesia's ideological values.

B. Problem Formulation

This paper addresses two problems. First, how has Indonesian cyberspace law been constructed, particularly regarding data protection and cybersecurity? Second, how does Indonesia's cyberspace law legal-philosophical stance impact its implementation?

[17] Nor Shazwina Mohamed Mizan, *et. al*. "CNDS-Cybersecurity: Issues and Challenges in ASEAN Countries" (2019) 8 International Journal of Advanced Trends in Computer Science and Engineering 113; Farisya Setiadi, Yudho Giri Sucahyo, and Zainal A. Hasibuan, "An Overview of the Development Indonesia National Cyber Security" (2012) 6 International Journal of Information Technology & Computer Science 108; Hammam Riza and Moedijono, "Country Paper In Cybersecurity Initiative, National Cybersecurity Policy & Implementation for Government of Indonesia" (2006); Maulia Jayantina Islami, "Challenges in The Implementation of National Cybersecurity Strategy of Indonesia from The Global Cybersecurity Index Point of View" (2017) 8 Jurnal Masyarakat Telematika dan Informasi 137; Sarah Safira Aulianisa and Indirwan Indirwan (n 6); Jirapon Sunkpho, Sarawut Ramjan, Chaiwat Oottamakorn (n 4).

[18] *See* Muhammad Firdaus, "A Review of Personal Data Protection Law in Indonesia" OSF Preprints (2020). Jihyun Park and Dodik Setiawan Nur Heriyanto, 'In Favor of Immigration Data Protection Law in Indonesia and Its Utilization for Contact Tracing' (2022) 4 (1) Prophetic Law Review 1.

[19] *See* Hardianto Djanggih and Nurul Qamar, "Penerapan Teori-teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime) (2018) 13 Pandecta 10; Miftahur Rokhman Habibi and Isnatul Liviani (n 6); Tamarell Vimy and others, "Ancaman Serangan Siber pada Keamanan Nasional Indonesia" (2022) 6 Jurnal Kewarganegaraan 2319; I Nyoman Sukayasa and Wayan Suryathi (n 7).

C. Methodology

This research applies a normative-doctrinal methodology to analyze Indonesia's existing cyberspace legal framework. It criticizes the substantive approaches that are used by the Indonesian government to regulate cyber activities such as privacy and data protection, information, and electronic transaction, antipornography, and cybersecurity. This article contextualizes Indonesia's existing cyberspace legal framework based on the two most common approaches in cyberspace governance, cyber liberalism, and protectionism. This research explains where Indonesia is positioned regarding its cyberspace governance.

D. Discussion and Result

1. The Construction of Regulations Governing Data Protection and Cybersecurity in Indonesia

i. Understanding cyberspace

The term 'cyberspace' was originally invented to describe 'the emerging world,'[20] which conveys a novel environment and dimension, the inverse of physical reality. At a quick glance, cyberspace may merely seem like a personal computer connected to the internet. However, if a broader outlook is taken, elements of political, social, economic, cultural, and financial networks constitute their own portions in cyberspace.[21] Hence, cyberspace does not only consist of hardware, but a series of symbolic definitions that constitute a network of ideas.[22] Today, cyberspace is considered a domain for mankind and technology, involving people across nations, fusing cultures and languages from people of all ages and occupations, supplying and demanding information, including a worldwide network of computers interconnected by means of telecommunication infrastructures enabling information to be processed and transmitted digitally.[23] Such an environment encompasses various components, including the system of 'node' computers and web servers scattered throughout the world and intermediaries such as system operators and service providers.[24] In this sense, cyberspace is a larger homogeneous space than merely what the internet is. As

[20] William Gibson, *Neuromancer* (Ace Science Fiction Books, 1984).
[21] David Bell, *An Introduction to Cybercultures* (Routledge, 2001).
[22] David Bell (n 21).
[23] T Fuenters-Camacho, "Introduction: UNESCO and the Law of Cyberspace" in Bruno Padirac (ed), *International Dimensions of Cyberspace Law* (1st edition, Ashgate Publishing Company, 2000).
[24] T Fuenters-Camacho (n 23).

Lessig describes it, the cyberspace is built on top of the internet, and gives a richer experience.[25] It is rapidly expanding with various forms of digital interactions and communications.

The activities undertaken in cyberspace ignore territorial boundaries and challenges the traditional limitations that typically link entities involved in electronic communications and the rules governing their responsibilities.[26] Cyberspace exists for digital participants to operate in it. In a narrow sense, cyberspace is a space where electronic entities interact.[27] However, from a broader perspective, cyberspace does not consist of only one distinct model, but many cyberspaces with numerous and various models from the real world that are replicated in computer-mediated communications.[28] Cyberspace is a conceptual space with information and communication technologies rather than the technology itself.[29]

The existence of cyberspace relies on its nonconceptual geography. The author found that the structure of cyberspace geography consists of at least three areas, technical geography, spatial geography of users, and economic geography of production.[30] Technical geography deals with computing elements such as nodes of information and bandwidth.[31] Spatial geography relates to the users' positions globally or within social and physical networks. Economic geography of production is for example areas such as Silicon Valley or the manufacturing base of Southeast Asia. Whittaker believes that the geographies of cyberspace are much more complex, involving notions of identity and community, notions of geometry, space and architectural forms, and the series of connected files and retrieval procedures that exists in it.[32]

Considering its international nature, the notion of 'space' in cyberspace does not always strictly translate to a metaphorical sense. Cyberspace represents a larger range of cultural, social, and political networks—in which a particular communication system exists—known as the internet. This wider virtual domain

[25] Lessig Lawrence, *Code, and Other Laws of Cyberspace (*Basic Books, 1999).
[26] Maria Anna, "An International Legal Instrument for Cyberspace? A Comparative Analysis with the Law of Outer Space" in Bruno Padirac (n 23).
[27] Maria Anna (n 26).
[28] Maria Anna (n 26).
[29] William Gibson (n 20).
[30] Manuel Castells, *The Internet Galaxy* (Oxford University Press, 2001).
[31] Manuel Castells (n 30).
[32] Jason Whittaker, *The Cyberspace Handbook* (Routledge, 2004).

constructs the relationships among agents and participants in the real world.[33] The substantiality of human relationships in the virtual world act as much as (even beyond) what it is in the real world. The amity among individuals is created through information about or knowledge of others equal to traditional physical interactions.[34] This proves that the existence of cyberspace, and activities that are conducted therein, translate to real repercussions.

The convergence of computer and telecommunications technologies is manifested in the communications network (a global network comprising many individual networks), known as the internet, is also described as "self-healing."[35] This is because computers are interconnected in such a way that transmissions can be rerouted around inoperable or congested nodes of the network. The messages are also broken into packets rather than being forwarded as a single data stream for transmission.[36] Each packet takes a different route and will still be received and reassembled at the destination computer.[37]

As a part of cyberspace, the internet consists of a global network linked together by wires of telecommunication technologies (copper, coaxial, and fiber optic cable, as well as radio and microwaves).[38] Each linked computer resides within a nested hierarchy of networks, from the local area to service provider, to regional, national, and international telecommunication networks. Such links vary in terms of their speeds and capacities, which can also be permanent, transient, or even dial-up connections.[39] Almost all networks allow connections to other networks by employing common communication protocols to form a global system (internet protocol).[40] Within each network space, individuals are able to access information stored on other computers, exchange e-mails, engage in an 'online communities,' take part in real-time conferences, play video games, explore virtual worlds, run software, and conduct electronic commerce.

[33] Jason Whittaker (n 32).
[34] Jason Whittaker (n 32).
[35] Yee Fen Lim, *Cyberspace Law* (2nd edition, Oxford University Press, 2007).
[36] Dennis Broeders, *The Public Core of the Internet: an international agenda for internet governance (*Amsterdam University Press, 2015) 10.
[37] Dennis Broeders (n 36).
[38] Martin Dodge and Rob Kitchin, *Mapping Cyberspace* (Routledge, 2001) 2.
[39] Martin Dodge and Rob Kitchin (n 38).
[40] Ed Krol and Ellen Hoffman, 'What Is the Internet?' (1993).

Given its complex nature, it is almost impossible to determine the size of the internet. It is reasonable however to point out the extraordinary growth the internet has experienced since 1981. Back then, fewer than 300 computers were linked to the internet, and the number has grown exponentially, linking over 1,000,000 computers.[41] As of 2020, there are over 4.4 billion internet users worldwide.[42] Some computers and computer networks that make up these numbers belong to governments, public institutions, and non-profit organizations. This has resulted in a decentralized, global medium of communications that links people, institutions, corporations, and governments around the world making up cyberspace.[43] Consequently, there is no centralized[44] storage location, control point, or communications channel for the internet, and it is not plausible for anyone to control all the information conveyed on the internet.[45]

That information is stored, accessed, and developed in the World Wide Web (WWW). The WWW consists of multimedia data such as texts, static graphics, sound, animation, clips, and virtual spaces which are stored as hypermedia documents. The WWW can be accessed using a browsing program such as Internet Explorer, Netscape, or some of the more sophisticated and popular ones currently, Safari, Mozilla Firefox, and Google Chrome. Thus, the WWW is a powerful medium for exploring related subjects and needs of mankind to easily surf for documents with one click of a button without concern for their specific location on the network or in a specific geographic space.[46]

The global link for receiving and dispatching data through connected networks is the object of examination of this research. This understanding of cyberspace is articulated to contextualize a broader perspective of what is meant to be governed. Thus, the following section elaborates on how Indonesia's cyberspace is regulated.

[41] Yee Fen Lim (n 35).
[42] Yee Fen Lim (n 35) 5.
[43] Yee Fen Lim (n 35) 6.
[44] Cocca A. Aldo "The Advances in International Law through the Law of Outer Space" (1981) 9 Journal of Space Law 27.
[45] Yee Fen Lim (n 35).
[46] Martin Dodge and Rob Kitchin (n 38).

ii. Indonesia's cyberspace legal framework

In general, Indonesia has an almost-complete regulatory framework governing its cyberspace. If one were to categorize the two primary scopes that shall be governed in cyberspace (data protection and security), it would be fair to say that there are laws governing them. It is a matter of where and how they are regulated which causes confusion. In this section, the primary laws that regulate Indonesia's citizens' activities on the internet will be explained. This includes the 1945 Constitution, the Law on Electronic Information and Transactions, the Law on Personal Data Protection, the Law on Anti-pornography, and the existing legal framework on cyber security.

The 1945 Constitution of Indonesia acts as the fundamental basis establishing the *rechtstaat* (rule of law) and must be referred to by all legislation. There are unity and statutory arrangements consisting of various components that are mutually dependent on each other others in the legal system in Indonesia, which were built to achieve the goals of the state and is guided by the principles and ideals of national law enshrined in the 1945 Constitution. The 1945 Constitution serves as a primary tool for protecting the national interest of Indonesia. In the Constitution, five values known as the *Pancasila* is contained namely: the value of divinity, humanity, unity, democracy, and justice. These five values are stated in the opening part of the 1945 Constitution paragraph IV. Pancasila refers to a citizenship theory and structural functionalism which can be said to be an idea of building good citizenship, also the result of community agreement, shared social values that contribute to life, and can be a source of social integration.[47] As mandated by the 1945 Constitution, the Indonesian government has to maintain those national values while attempting to adapt to the increasing use of information technology and communication. Adaptation is performed through creating laws to fill in the relevant legal gaps and sustaining future activities, is no easy feat. Such values to which we will see might contradict the aims of the cyberspace freedom. There are limitations set by the 1945 Constitution that cannot be negotiated. Some values concerning religion, culture, and humanity continue to restrict the activities of Indonesian citizens in cyberspace.

[47] G Ritzer, *Sosiologi Ilmu Pengetahuan Berparadigma Ganda* (Rajawali Press, 2004).

Law No. 11 of 2008 on Information and Electronic Transaction was established as a legal umbrella encompassing Indonesia's cyber affairs. It was based on the consideration of national development, globalization of information, and the development of information and communications technology (ICT). The law also aims to secure public spaces to remain conducive to the bigger goal of achieving digital democracy. Some principles that are established for the regulation of ICT includes legal certainty, benefits, prudence, good faith, and freedom to choose technology or technology neutrality. The last principle is worth emphasizing. From the perspective of legislation, the principle of 'technology neutrality' drives towards regulating the effects of technology and not the technology itself. This is aimed at regulations to not having a negative pullback towards the development of technology.[48] In other words, the government, policymakers, corporations, and individuals are not bound by particular types of technology. From this instance, it can be inferred that 'freedom-driven' values are incepted within Law No. 11 of 2008.

Law No. 11 of 2008 applies to individuals who are within the jurisdiction, as well as outside of Indonesia and having a legal impact within the jurisdiction of Indonesia or is detrimental to the state's interest.[49] As we see later in other regulations, a similar approach to apply the principle of extraterritoriality, a key to accommodating the borderless nature of cyberspace.

Law No. 11 of 2008 regulates a variety of activities, capturing many aspects of ICT. Such activities include preserving electronic information, records, signature, electronic certification and systems, electronic transactions, domain names, intellectual property rights and privacy rights, and prohibited acts. Prohibited acts includes illegal distribution/transmission of electronic information and/or records, dissemination of false and/or misleading information, electronic information/records containing violent threats, unlawful access to computers and/or electronic systems, illegal interception/wiretapping, and the alteration of records of another person or the public. From its content, it is difficult to pinpoint the focus of the law. On one hand it focuses on cyber related crimes, and on the other it also tries to prevent illegal content and wrongful uses of the internet. For

[48] Bert-Jaap Koops, 'Should ICT Regulation Be Technology-Neutral?' (25 July 2006) <https://papers.ssrn.com/abstract=918746> accessed 29 March 2023.

[49] Law No. 11 of 2008 on Electronic Information and Transaction (n 9).

most of its prohibition, it is obvious to see a conflict between the government's endorsement for the openness of its cyberspace, while on the other side it still wishes to strictly limit on what activities can be conducted by its citizens.

Similar to Law No. 11 of 2008, Law No. 27 of 2022 on Personal Data Protection is fundamentally constructed based on the 1945 Constitution. It is stipulated that personal data protection is the right of citizens. The law was established to increase the effectiveness of personal data protection. Consisting of 76 articles, this law acts as the basis for data protection in Indonesia to supersede the previously fragmented legal sources. Law No. 27 of 2022 governs the relationship between data controller, data processor, and data subject with respect to the collection, processing, analyzing, storing, fixing, updating, deleting, and terminating personal data. The law differentiates between personal and public data; different treatments may be applied. It also regulates the rights and obligations of the parties involved at each of those processes. Other aspects that are also governed by Law No. 27 of 2022 includes the transfer of personal data, the obligation to appoint a data protection officer, international cooperation, dispute settlement, as well as administrative and criminal sanctions for violation of the provisions therein. Overall, the law is comprehensive enough to act as a legal foundation for protecting Indonesian citizens personal data. The law is based on the principles of protection, legal certainty, public interest, prudence, equality, responsibility for confidentiality. Unlike Law No. 11 of 2008, Law No. 27 of 2022 does not mention any principles protecting the freedom of its citizens in terms of utilizing the internet, namely the right to free speech and freedom of expression.

Furthermore, there is an issue concerning the right to privacy, the right to be forgotten, and freedom of expression. Particularly, for the rights of personal data subjects," which includes the ability to control one's personal data using electronically or non-electronically registered requests to data controllers. However, terminating, deleting, withdrawing, and objecting to data use may only be requested if it does not contradict the interests of national security and defense, law enforcement, general interests of the public, state administration, the interests of financial service sectors, and research. One may argue that such limitations contradict the right to be forgotten, a principle that is substantially protected by

the United States and the European Union.[50] The ability of individuals to erase, limit, delete, or correct misleading personal information on the Internet that is embarrassing, or irrelevant are considered to be as important as its creation. Such right falls under the right to privacy and the right to freedom of expression.

Law No. 44 of 2008 on Antipornography is legislation which took 10 years to enact. During its deliberation, the debate on regulating pornography in Indonesia was highly disputed. Debates were mostly about the costs and benefits of assessing, interpreting, and formulating the terms and meanings of pornography.

The construction of this law comes from the 1945 Constitution and the Criminal Code. While most of its penal sanctions are rooted in the criminal code, the law does not differentiate the medium and the kinds of pornographic contents, whether visual, written or audio. It also does not distinguish between the matter of distribution whether by virtual or conventional. Some of the prohibited acts include funding or facilitating the production or the distribution, posing or acting as a model of pornography, downloading, lending, showing, viewing, possessing, saving pornographic contents, providing service to pornographic activities, producing, duplication, distribution, and/or selling pornographic contents. Philosophically, such prohibitions contained in the law are related to issues of freedom and human rights. The philosophical basis of the law refers to the same values contained in the 1945 Constitution and Pancasila. The country's belief of the Supreme and almighty God, admiration, and respect of the dignity and worth of humans, diversity, the rule of law, non-discrimination, and the protection of citizens are non-negotiable. With this, the main purpose of the law is to maintain social order of the community and community ethics, supremacy of privacy, priceless value of God, and admiration and respect of the dignity and worth of humans as well as to cultivate and instruct a moral and ethnic community. It is perceived that the construction of such law is by necessity for the protection of the citizens from pornographic content, particularly for children and women. The law is also aimed at preventing the commercialization of sex within the community. It is prescribed within the law the protection of children is every

[50] Michael Kelly and David Satola, "The Right to Be Forgotten" (2017) University of Illinois Law Review 1.

adult's responsibility. Such responsibility is also shared between the role for government, social institutions, educational, religions institutions, families, and/or the community for the subordination, alignment, and social dignification, physical health and mental health of child victims or subjects/performers in pornography. Conclusively, contents that are related to anywhere near the exposure of pornography or indecent depiction of sex are strictly prohibited. Thus, there is no room for an individual to sexually express themselves publicly or virtually in cyberspace.

The reliance on cybersecurity systems is highly important for protecting Indonesia from threats to networks, devices, and organizational and personal information. The major data breach incidents of the past 1.5 years, targeting government institutions, healthcare providers, security agencies, general elections, and e-commerce are evidence of Indonesia's weak cyber security system. Currently, Indonesia does not have any specific regulation for cyber security. Most of the laws that touch upon this issue are fragmented and overlapping. The enactment of Law No. 27 of 2022 has contributed to covering one of the security weaknesses, but it is still insufficient and there is an urgency to immediately enact a specific law on cyber security.

As personal data is one of the objects protected under cybersecurity mechanisms, it is quintessential that networks, computers, programs, and data are protected from attacks and unauthorized access. Cyber security measures also underpin critical infrastructure that protects data and safeguards personal information. Despite the absence of a specific law for cybersecurity, Indonesia has in fact a few legal measures in place. These measures are included in the Law on Telecommunication, the Law on Information and Electronic Transaction, the Law on Broadcasting, the Law on the Openness of Public Information, the Criminal and Procedural Code, the Antipornography Act, the Copyright Act, the Consumer Protection Act, and technical and procedural measures such as the National Standard on Security Management (ISO 270001) (SNI ISO/IEC 27001:2009). Several institutions who are tasked with overlapping functions for cyber security also exist, including the Ministry of Communication and Information Technology (Kominfo), State Intelligence Agency (BIN), and National Standardization Body (BSN).

Cyber security regulations in Indonesia fall under the authority of the Coordinating Ministry for Political, Legal and Security Affairs of the Republic of Indonesia (Kemenkopolhukam). Through the Decree of the Coordinating Minister for Political, Legal and Security Affairs Number 24 of 2014 concerning the National Cyber Information Security and Resilience Desk (DK2ICN). The institution authorized to handle cybercrimes is the police, through its cybercrime division. Together with the Ministry of Communication and Informatics, through the directorate of information security for law enforcement of the Law No. 11 of 2008, institutions that play a role in managing information obtained by the public and have the right to control internet content. The authority to investigate cases can be carried out by two parties, police investigators or civil servant investigators (PPNS) of Kominfo. The handling of cases depends on where the case is reported. Most accounts reported to cybercrime are the result of reports from the public.

2. The Legal-Philosophical Stance of Indonesia's Cyberspace Law and The Impact of Its Implementation

i. The freedom and protectionist approaches

To contextually describe Indonesia's cyberspace governance, it is important to first understand the two common approaches that are implemented by states. It is worthy to note that there is no single right or wrong answer to these approaches, nor is there a legal basis that binds states. However, as political spectrums categorize certain state's governance, it can be used as a similar reference for the governance of cyberspace. There are at least two approaches the liberal, or '*freedom'* approach, and the protectionist approach.

Cyber freedom mainly comprises the right to internet access, freedom of expression and information, and freedom from internet censorship. Cyber freedom refers to an approach to regulating cyberspace that opposes state monopolies over cyberspace regulation making.[51] A compelling argument for this concept could be argued by the nature of the most known cyberspace instrument, the internet. According to Lessig, the internet was not designed for information

[51] Richard A Spinello, "Ethics in Cyberspace: Freedom, Rights, and Cybersecurity" in Ali E Abbas (ed), *Next-Generation Ethics: Engineering a Better Society* (Cambridge University Press, 2019).

concealment, but rather for openness and research.[52] Meanwhile, many states believe that limiting cyberspace is the way forward. By exercising jurisdiction over cyberspace facilities, data governance, and cyber operations, the sovereign will be able to protect the cyberspace from harm and unnecessary chaos.[53] In other words, these limitations constitute a cyber protectionist approach. Cyber protectionism is a broad term that refers to a wide range of barriers to digital trade (e-commerce) and cross-border data flows,[54] with examples such as censorship, filtering, localization measures and regulations to protect privacy.[55] When observing the legal framework for cyberspace, a division is made between 'cyber liberals' and 'cyber protectionists.' The prior opts for complete freedom and unlimited use and exploitation of cyberspace, while the later prefers the suppression of such freedoms. Cyber freedom favors a multi-stakeholder approach, while the cyber protectionism prefers government centered authority.

To better comprehend these two approaches, the author contextualizes these approach using the practices conducted by United States and China. The history of cyber freedom is laid in the foundation of the internet where, in the 1960s, researchers from the US military established the foundation for the internet.[56] Since then, universities, private institutions, and private entities have joined in a haphazard, organic, and decentralized manner.[57] However, countries, including the US, have played a huge role in regulating it despite its inclusive nature.[58] Multi-stakeholder governance is popular among countries in which libertarian ideas are popular. Its factions include Free Culture, Global Public Good (GPG),[59] Maximalist, and Anti-Marketization.[60] Aside from the US, countries like the

[52] Richard A Spinello, "Code and Moral Values in Cyberspace" (2001) 3 Ethics and information technology 137.

[53] Philip G Zimbardo, "The Human Choice: Individuation, Reason, and Order versus Deindividuation, Impulse, and Chaos" (1969) 17 Nebraska Symposium on Motivation 237.

[54] Susan Ariel Aaronson (n 13).

[55] US Commission, "Digital Trade in the U.S. and Global Economies" (2013).

[56] Zhixiong Huang and Kubo Mačák, "Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches" (2017) 16 Chinese Journal of International Law 271.

[57] Zhixiong Huang and Kubo Mačák (n 56).

[58] Zhixiong Huang and Kubo Mačák (n 56).

[59] Andrew N Liaropoulos, "Cyberspace Governance and State Sovereignty", in *Democracy and an Open-Economy World Order* (Springer International Publishing, 2017).

[60] Jean Marie Chenou, "From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi-Stakeholderism, and the Institutionalisation of Internet Governance in the 1990s" (2014) 11 Globalizations 205.

United Kingdom (UK), Canada, and the European Union (EU) are known proponents of the multi-stakeholder regime.[61]

The popularisation of multi-stakeholder governance has gained global recognition in UNGA Resolution, 57/239 of 2002. Known stakeholders include "*…governments, businesses, other organizations and individual users who develop, own, provide, manage, service and use information systems and networks*….".[62] Multi-stakeholder governance is famous for its inclusive and representative principles where stakeholders can establish norms and set standards and define penalties and repercussions for violations. Furthermore, recent developments within the UN discussed the roles of these stakeholders. Such roles consist of stakeholders as influencers of opinions, problem solvers, contributors, decision-makers, sponsors of national engagement, and whistle-blowers.[63] Aside from the UN, the US also utilizes a multi-stakeholder approach in its 'Internet Freedom' diplomacy to increase the protection of human rights in cyberspace.[64]

Further proof of the US's cyber freedom governance shows that citizens of the US are free to criticize their government. The US government does not take punitive action and even supports the medium of cyberspace as a place of criticism.[65] Indeed, the First Amendment of the US Constitution guarantees freedom of expression except for fraud, obscenities, defamation, and incitement.[66] US is even laxer in cyberspace, as the US government immunizes content providers (namely YouTube and Facebook) from the actions of their users should consider an exception to freedom of expression occurs.[67]

Unlike cyber freedom, what we've termed as the cyber protectionist concept is where countries must exclusively govern cyberspace without any external interference. Such an idea is popular in China, where it relies on two

[61] Zhixiong Huang and Kubo Mačák (n 56) 2917).

[62] Andrew N Liaropoulos (n 59) 20.

[63] Bruno Lété, "Shaping Inclusive Governance in Cyberspace" <https://www.gmfus.org/news/shaping-inclusive-governance-cyberspace>.

[64] "Internet Freedom" <https://www.state.gov/wp-content/uploads/2019/03/Internet-Freedom.pdf>.

[65] "Internet Freedom" (n 64).

[66] Fernando Nuñez, "Disinformation Legislation and Freedom of Expression" (2020) 10 UC Irvine Law Review 784.

[67] Fernando Nuñez (n 66).

principles; unwanted influence in a country's cyberspace must be banned and shift internet multistakeholder governance to an international forum.[68]

The core philosophy in applying sovereignty to cyberspace is similar to the traditional notions of sovereignty. Proponents of cyber protectionism argue for using state jurisdiction to govern cyberspace facilities, carrying data, and operations of data in cyberspace where state judicial and administrative institutions can exercise their power over cyberspace.[69] Hence, every sovereign state has the right and duty to not interfere with other states' cyberspace and protect its cyberspace against aggression.[70] Cyber protectionists are composed of several factions, including reformists, neoliberal proponents of cybersecurity, and sovereigntists.[71]

Proponents of the cyber protectionist concept have emerged as a reaction to the cyber freedom multistakeholder approach, including countries such as China, Russia, Cuba, Iran, Saudi Arabia, Bahrain, United Arab Emirates (UAE), Iraq, and Sudan.[72] Countries like China view the multistakeholder approach as defective in the platform with limits to authorization, function, and interest equity.[73] Furthermore, according to the protectionist concept, the multistakeholder approach framework is lacking in both design and coordination.[74] Hence, because of perceived defects in the cyber freedom concept, some countries prefer a protectionist attitude to cyberspace as the way forward.

Current developments of the cyber protectionist agenda are domain name jurisdiction, data ownership rights, big data, different judging legality principles, and cyber-attacks.[75] Yet, there is a concern about the nature of cyber protectionism. Should the role of countries become too big, this may disturb day-to-day social life due to the current interconnected nature of this globalized world. Potential problems include the defunct Autonomous Systems (AS) due to varying state regulations, removal of transnational organizations from domain administration, the emergence

[68] Niels Nagelhus Schia and Lars Gjesvik, "China's Cyber Sovereignty" Norwegian Institute of International Affairs Policy Brief (2017).
[69] Binxing Fang, *Cyberspace Sovereignty* (Springer, 2018).
[70] Binxing Fang (n 69).
[71] Jean Marie Chenou (n 60).
[72] Zhixiong Huang and Kubo Mačák (n 56).
[73] Zhixiong Huang and Kubo Mačák (n 56) 35.
[74] Zhixiong Huang and Kubo Mačák (n 56) 35.
[75] Binxing Fang (n 69).

of national online checkpoints, the overabundance of certification demand, and strict data localization requirements.[76] However, there are a few concerns over approaches by the protectionist such as measures regarding cyber espionage, intrusive authoritarian policies, and complete media control.

Thus, it could be inferred that from these two approaches, cyber freedom opts for the liberalization and openness of cyberspace to everyone: with instances of involving a multi-stakeholder approach for its governance and setting no limitations to user's activities. Meanwhile, the cyber protectionism focuses on a state's authority to exclusively govern the cyberspace and set limitations on what its citizens can and cannot do on the cyberspace. Clearly, depending on what approach is taken, the consequences and effectiveness of cyberspace governance will differ. This research does not go to such extent, but rather to merely evaluates Indonesia's position between the two, from several fundamental regulations.

ii. Indonesia's position: between freedom and protection

It is believed that the core values which should be embedded in cyberspace must always refer to equality and inclusivity despite any differences in a state's governance model. Since 2016, it has been reported by Freedom House that Indonesia's internet freedom status is 'partly free.'[77] Freedom House evaluates a nation's place on the spectrum based on the obstacles to access, limits on content, and violations of users' rights. With a population of over 250 million, Indonesia has 22 percent internet penetration in 2016, and a staggering 73.7 percent in 2022. The number of internet users between 2021 and 2022 has increased by 2.1 million.[78] Despite the increase in such numbers, Indonesia still applies consistent measures in terms of ICT applications blocking, content filtering, and criminalization of ICTs and individuals.

To assess Indonesia's position, the author analyses the two primary aspects of cyberspace governance, privacy and security. First, it is understood that in the aforementioned regulations, the government is trying to regulate access and content that are deemed to be 'negative.' Such term has been frequently used to

[76] Zhixiong Huang and Kubo Mačák (n 56).

[77] Freedom House, "Freedom on the Net 2016" (2016) <https://freedomhouse.org/sites/default/files/FOTN%202016%20Indonesia.pdf>.

[78] Freedom House, "Freedom on the Net 2022" (2022).

describe content of a pornographic or defamatory nature, as well as contents that are contradictory to social norms. Law No. 11 of 2008 sets a broad spectrum of what it considers a prohibited act. The prohibitions towards illegal distribution and/or transmission of electronic information and records, as well as dissemination of false and leading information seem to overshadow the objectives of the law governing the management of electronic documents, transactions, intellectual property, and privacy. This affects the public's perception of the law as opposed to fundamental of human rights, particularly in the context of the freedom of speech and expression. Furthermore, while it may seem that Law No. 11 of 2008 opens opportunities for public participation, the role of the public is extremely limited. The only way that the public can play the role of improving the information technology usage through the law is via public institutions by ways of consultation and mediation. Thus, the only liberalizing aspect of Law No. 11 of 2008 could only be found at the freedom of technology neutrality which benefits stakeholders more than the public.

Second, in terms of data protection and the right to privacy, Law No. 27 of 2022 displays a significant contrast of freedom compared to Law No. 11 of 2008. This might be due to the substantial influence of the General Data Protection Law of the European Union (GDPR). Some similar aspects that Law No. 27 of 2022 has to the GDPR include consent, definition and scope of data controller and processor, and the creation of data protection officers. Theoretically, the principles, scope of application, rights and obligations between stakeholders and individuals are equally divided. The law does not substantially put individuals right to access and utilize the cyberspace to be one sided in terms of one's prerogative right to their personal data. The only limitation that such freedom might receive are in terms of protecting public interest, which is a generally broad and arguably intentionally vague term.

Third, outside of content moderation that are either explicitly or implicitly regulated in Law No. 11 of 2008 and Law No. 27 of 2022, the Law on Antipornography acts as a non-negotiable cornerstone of protecting Indonesian religious and cultural values. Pornography remains the most blocked category of content, with nearly 1.1 million sites blocked between August 2018 and July

2021 according to Kominfo.[79] Despite Law No. 11 of 2008 guidelines for the blocking of web content, it does not appear to have a transparent and accountable blocking policy or procedure. According to Freedom House, civil society and cultural groups challenged the law before the Constitutional Court in 2009 for its narrow and obscure definition of pornography and pornographic content, which includes LGBTQ+ content and folk traditions that expose the female form, such as the Jaipongan folk dance from West Java and Papuan traditional clothes. The Court upheld the law.[80]

Fourth, concerning cyber security, Indonesia still faces challenges of cyberattacks, cybercrime, cyber prostitution, cyber propaganda, cyber terrorism, and cyber warfare.[81] As Indonesia's legal framework for cybersecurity is scattered across various government institutions, agencies, and ministries, it creates difficulties for parties to coordinate and take effective response when an incident has occurred. The overlapping of regulations and lack of clear coordination between institutions urges the need for an umbrella law to integrate the efforts for creating an effective cybersecurity system. This is to prevent and minimize risks of threat such as unauthorized access, illegal content, data forgery, cyber espionage, cyber extortion, and cybercrime. The Indonesian government and other stakeholders need to have a uniform understanding for the management of security in cyberspace. Also, the awareness of threat and coordinated responses requires a firm legal basis for the relevant parties to act.

iii. The way forward?

The borderless nature and flexibility of cyberspace requires a balance in its governance, that neither prevails absolute freedom nor authoritarian restraints. The regulatability of cyberspace refers to the ability of a government to regulate the behavior of its citizens on the internet. Internet governance includes issues directly related to the technical administration of electronic resources, including private entities, as well as all actions performed by state authorities using legal

[79] S Fikria, "2.5 Million Internet Content Blocked, Majority of Porn Sites" in Radar Solo Jawapos (2021).

[80] Olivia Rondonuwu, "Indonesia's Constitutional Court Defends Pornography Law" (2010) <https://www.reuters.com/article/us-indonesia-pornography-idUSTRE62O28R20100325>.

[81] Sarah Safira Aulianisa and Indirwan Indirwan (n 6).

instruments and international organizations exerting a direct impact on activities performed using the electronic medium, including those outside a regulating state.

The preeminent starting line is obviously the right to privacy and freedom as fundamental human rights. The right to privacy inhibits the government and private actions from invading the privacy of individuals where they are free from interruption or intrusion and can control the time and manner of the disclosure of their personal information. Freedom in cyberspace, on the other hand, encompasses many different types of freedoms, with freedom of expression as one of the core freedoms in cyberspace. Despite the utmost importance of privacy rights and freedom of expression, limitations to both must be drawn clearly.

Cyberspace promotes equality and inclusivity, as seen in the threshold upheld by United Nations,[82] as well the characteristics cyberspace itself which helps by providing access to information for every of its users. The notion of equality and inclusivity in cyberspace, however, will of course result in perpetrators who violate such rights, thus committing cybercrimes. Cybercrimes vary from hacking, spreading hate, and misusing personal information to distributing child pornography, grooming and terrorism.[83] Penalties for cybercrimes are also similar in many countries including large fines, imprisonment for a number of years depending on the severity of the cybercrime, and also the obligation to provide restitution to the victims in some countries the United States, and reparations in Europe.[84]

Information is closely related to freedom of opinion, conveying ideas, constitutional rights. These principles are the pillars of law in a democratic country, all of which are guaranteed by the 1945 Constitution. Although freedom is not absolute, care must be taken in applying Law No. 11 of 2008. Prioritizing elements of the regulatory nature of Law No. 11 of 2008 (rather than the element of coercion). The legislators understand very well that repressive elements can interfere with freedom of opinion and expression. The National Police Chief decided to issue a circular that shifts the process of implementing Law No. 11 of 2008 into restorative justice. According to him, in criminal cases, it is known as

[82] International Telecommunication Union, "ICTs for a Sustainable World #ICT4SDG" (2021) <https://www.itu.int/en/sustainable-world/Pages/default.aspx>.

[83] Government of the Netherlands, "Forms of Cybercrime" (2021) <https://www.government.nl/topics/cybercrime/forms-of-cybercrime>.

[84] Jean-Claude Juncker, "Strengthening Victims' Rights: From Compensation to Reparation for a New EU Victims' Rights Strategy 2020-2025" (2019).

peace efforts (between the victim and the perpetrator). Restorative justice has a strong foundation for our society. That is, it has a strong basis of cultural and sociological aspects.

In terms of cybersecurity, it is urgently needed that deliberation on the draft Bill on Cybersecurity and Resilience must involve public participation. The bill must provide an overview of Indonesia's long term cyber strategy and having consistency between the principles, aims, scope, and applicability. The National cybersecurity strategy must also include legal remedies, technical efforts conveying standards and operations, organizational and institutional structuring of cybersecurity subscribes, capacity building, human resource, and international cooperation. Such strategy must also consider the most relevant threats that Indonesia has been facing as its priorities.

E. Conclusion

From a quick glance, the cyberspace may merely seem like a personal computer connected to the internet. However, if a broader outlook is taken, elements of political, social, economic, cultural, and financial networks constitute their own portions in the cyberspace. The borderless nature and flexibility of cyberspace requires a balance in its governance, that neither prevails absolute freedom nor authoritarian restraints. The regulatability of cyberspace refers to the ability of a government to regulate the behavior of its citizens on the internet. Internet governance includes issues directly related to the technical administration of electronic resources, including private entities, as well as all actions performed by state authorities using legal instruments and international agreements.

This article has discussed the two major approaches at governing cyberspace which are the freedom and protectionist movements. The characteristics of both approaches have been contextually put to the governance of cyberspace in Indonesia. It is found that Indonesia's position is somewhere in between. On one side, Indonesia realizes that the rapid development of technology will always demand its law to adapt and gradually open more opportunities for its citizens to access and benefit from. On the other side, national and public interest is still highly prioritized which are evident from the principles, articles of laws such as the Law on Information and Electronic Transaction, Law on Personal Data Protection, Law on Antipornography, and the cybersecurity legal framework.

Although the constitution and other regulations ostensibly allow free speech, in practice this freedom is regularly restricted. Freedom of expression and other fundamental rights are protected by the Law on Human Rights, which was enacted shortly after the democratization process in 1998; the Second Amendment to the Constitution, which was passed in 2000, strengthened these safeguards. Despite the protections of the freedom of speech and the right to freely seek out information and communicate in the constitution and several Indonesian cyberspace laws, its implementation is always adjusted to Indonesia's ideological values.

The constitution does, however, contain provisions that permit the state to restrict rights considering political, security, moral, and religious reasons. This language gives decision-makers a wide range of interpretation options and poses a difficult question to map out Indonesia's legal-philosophical foundation for cyberspace governance. Nevertheless, Indonesia has reached significant milestones in terms of pursuing an ever more complete, integrated, and harmonious cyberspace law.

References

Indonesian Legislations

Law No. 27 of 2022 on Personal Data Protection.
Law No. 11 of 2008 on Electronic Information and Transaction.

Books

Anna M, "An International Legal Instrument for Cyberspace? A Comparative Analysis with the Law of Outer Space" in Bruno Padirac (ed), *International Dimensions of Cyberspace Law* (1st edition, Ashgate Publishing Company, 2000).

Bell D, *An Introduction to Cybercultures* (Routledge, 2001).

Broeders D, *The Public Core of the Internet: an international agenda for internet governance (*Amsterdam University Press, 2015) 10.

Castells M, *The Internet Galaxy* (Oxford University Press, 2001).

Dodge M and Kitchin R, *Mapping Cyberspace* (Routledge, 2001) 2.

Fang B, *Cyberspace Sovereignty* (Springer, 2018).

Fuenters-Camacho T, "Introduction: UNESCO and the Law of Cyberspace" in Bruno Padirac (ed), *International Dimensions of Cyberspace Law* (1st edition, Ashgate Publishing Company, 2000).

Gibson W, *Neuromancer* (Ace Science Fiction Books, 1984).

Kittichaisaree K, *Public International Law of Cyberspace. Law, Governance and Technology Serie*s (Springer, 2019).

Lawrence L, *Code, and Other Laws of Cyberspace (*Basic Books, 1999).

Liaropoulos AN, "Cyberspace Governance and State Sovereignty", in *Democracy and an Open-Economy World Order* (Springer International Publishing, 2017).

Lim YF, *Cyberspace Law* (2nd edition, Oxford University Press, 2007).

Puyvelde D and Brantly A, *Cybersecurity: Politics, Governance and Conflict in Cyberspace* (Polity Press 2019).

Ritzer G, *Sosiologi Ilmu Pengetahuan Berparadigma Ganda* (Rajawali Press, 2004).
Spinello RA, "Ethics in Cyberspace: Freedom, Rights, and Cybersecurity" in Ali E Abbas (ed), *Next-Generation Ethics: Engineering a Better Society* (Cambridge University Press, 2019).
Whittaker J, *The Cyberspace Handbook* (Routledge, 2004).

Journals

Aaronson SA, "What Are We Talking about When We Talk about Digital Protectionism?" (2019) 18 World trade review 541.
Aldo CA, "The Advances in International Law through the Law of Outer Space" (1981) 9 Journal of Space Law 27.
Aulianisa SS and Indirwan I, "Critical Review of the Urgency of Strengthening the Implementation of Cyber Security and Resilience in Indonesia" (2020) 4 Lex Scientia Law Review 30.
Chenou JM, "From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi-Stakeholderism, and the Institutionalisation of Internet Governance in the 1990s" (2014) 11 Globalizations 205.
Djanggih H and Qamar N, "Penerapan Teori-teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime) (2018) 13 Pandecta 10.
Habibi MR and Liviani I, "Kejahatan Teknologi Informasi dan Penanggulangannya dalam Sistem Hukum Indonesia" (2020) 23 Al-Qānūn: Jurnal Pemikiran dan Pembaharuan Hukum Islam 400.
Huang Z and Mačák K, "Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches" (2017) 16 Chinese Journal of International Law 271.
Islami MJ, "Challenges in The Implementation of National Cybersecurity Strategy of Indonesia from The Global Cybersecurity Index Point of View" (2017) 8 Jurnal Masyarakat Telematika dan Informasi 137.
Johnson DR and Post D, "Law and Borders: The Rise of Law in Cyberspace" (1996) 48 First Monday 1367.
Kelly M and Satola D, "The Right to Be Forgotten" (2017) University of Illinois Law Review 1.
Mizan NSM *et. al*. "CNDS-Cybersecurity: Issues and Challenges in ASEAN Countries" (2019) 8 International Journal of Advanced Trends in Computer Science and Engineering 113.
Nuñez F, "Disinformation Legislation and Freedom of Expression" (2020) 10 UC Irvine Law Review 784.
Park J and Heriyanto DSN, 'In Favor of Immigration Data Protection Law in Indonesia and Its Utilization for Contact Tracing' (2022) 4 (1) Prophetic Law Review 1.
Post D, "Governing Cyberspace: Law" (2018) 24 Santa Clara High Tech. L.J. 883.
Setiadi F, Sucahyo YG, and Hasibuan ZA, "An Overview of the Development Indonesia National Cyber Security" (2012) 6 International Journal of Information Technology & Computer Science 108.
Spinello RA, "Code and Moral Values in Cyberspace" (2001) 3 Ethics and information technology 137.
Sukayasa IN and Suryathi W, "Law Implementation of Cybercrime in Indonesia" (2018) 8 Journal of Social Sciences and Humanities 123.
Vimy T and others, "Ancaman Serangan Siber pada Keamanan Nasional Indonesia" (2022) 6 Jurnal Kewarganegaraan 2319.

Wu TS, “Cyberspace Sovereignty? – The Internet and the International System” (1997) 10 Harvard Journal of Law & Technology 648.

Zimbardo PG, "The Human Choice: Individuation, Reason, and Order versus Deindividuation, Impulse, and Chaos" (1969) 17 Nebraska Symposium on Motivation 237.

Miscellaneous

Anjani NH, “Perlindungan Keamanan Siber di Indonesia” Center for Indonesian Policy Studies (2021).

Fikria S, "2.5 Million Internet Content Blocked, Majority of Porn Sites" in Radar Solo Jawapos (2021).

Firdaus M, “A Review of Personal Data Protection Law in Indonesia” OSF Preprints (2020).

Freedom House, “Freedom on the Net 2022" (2022).

"Internet Freedom" <https://www.state.gov/wp-content/uploads/2019/03/Internet-Freedom.pdf>.

Freedom House, "Freedom on the Net 2016" (2016) <https://freedomhouse.org/sites/default/files/FOTN%202016%20Indonesia.pdf>.

Government of the Netherlands, "Forms of Cybercrime" (2021) <https://www.government.nl/topics/cybercrime/forms-of-cybercrime>.

Krol E and Hoffman E, ‘What Is the Internet?’ (1993).

Koops B-J, ‘Should ICT Regulation Be Technology-Neutral?’ (25 July 2006) <https://papers.ssrn.com/abstract=918746> accessed 29 March 2023.

Riza H and Moedijono, “Country Paper In Cybersecurity Initiative, National Cybersecurity Policy & Implementation for Government of Indonesia” (2006).

Rondonuwu O, "Indonesia’s Constitutional Court Defends Pornography Law" (2010) <https://www.reuters.com/article/us-indonesia-pornography-idUSTRE62O28R20100325>.

Schia NN and Gjesvik L, "China’s Cyber Sovereignty" Norwegian Institute of International Affairs Policy Brief (2017).

Sunkpho J, Ramjan S, and Oottamakorn C, “Cybersecurity Policy in ASEAN Countries” Information Institute Conferences in Las Vegas (2018).

US Commission, “Digital Trade in the U.S. and Global Economies” (2013).

US Commission, “United States International Trade Commission” (2013).