Evaluating Legal Frameworks for Cybercrime in Indonesian Public Administration: An Interdisciplinary Approach

***Ichsan Anwary*[1]**
Universitas Lambung Mangkurat, Banjarmasin, Indonesia

Abstract
With the advancement of technology and the growth of the internet and cyber, many negative factors, such as cyberattacks and cybercrime, are on the rise and hinder the internet's and technology's positive use. Cybercrime is one of the worst factors significantly increasing in Indonesia today. Cybercrime is a criminal act that is prohibited in every country on the planet. The instances of cybercrime have harmed Indonesian computer users. The present study evaluates the legal frameworks and articles designed to control cybercrime issues within the Indonesian public administration. This study utilized a qualitative descriptive approach, along with an empirical judicial technique and statute approach analysis method. Documents about articles and legal frameworks in Indonesia were analyzed for data collection. The types and patterns of Cybercrime in Indonesia are outlined in Articles 27 to 35 of Law No. 11/2008. Chapter XI of Act No. 11/2008 describes the forms and patterns of violation of confidentiality and privacy. Based on the findings and discussion of the legal framework and analysis, recommendations are made to promote preventive measures, increase accountability, and reduce the communication divide between the government and Cybercrime-authoritative agencies. Along with the research limitations discussed in the study, the study has numerous theoretical and practical implications.

Keywords: Cybercrime, Articles, Legal framework, Public Administration.

Introduction
The advancement of digital technology has resulted in a substantial increase in criminal activity, and the ease of access to Internet services has presented law enforcement agencies and the legal system with formidable challenges (Abdulkadir & Abdulkadir, 2019). Increasing online communication experiences have led to a dramatic increase in illicit activity on the internet. The advent of digitalization affected individual conduct and social order. This digitalization and the provision of

[1] Faculty of Law, Universitas Lambung Mangkurat, Banjarmasin, Indonesia.
Email: ichsan.anwary@ulm.ac.id ORCID ID: https://orcid.org/0000-0002-4693-6467

substantial benefits increase the means for committing internet crimes or cybercrimes (Koto, 2021). Cybercrimes are rapidly expanding digital crimes that pose a serious hazard to the national security of numerous nations. Legislation is the most important factor research studies highlight in combating cybercrime (Khan et al., 2022). Multiple state and non-state actors pose a danger to cyberspace today. The global nature of cybercrime brings to light the issue of jurisdiction, sovereignty, and transnational investigation, which necessitates international cooperation between legislative bodies (Mittal & Sharma, 2017). According to Okutan (2019), cybercrimes are the fastest-growing crimes, and many nations worldwide have implemented penal and judicial systems to mitigate their effects. As Asia rapidly expands its global e-commerce market, many academics perceive increased cybercriminal activity. Cybercrime is increasing swiftly in ASEAN nations, which have become a hub for cybercriminals in recent years. To prevent cybercrimes in Asia, the relevant countries must develop cybercrime laws aligned with national standards (Chang, 2020).

Effective cybercrime regulations in Indonesia include Regulation No. 11 from 2008 concerning Electronic data and exchanges and Regulation No. 19 from 2016 concerning Corrections to rules. Moreover, the processes to eliminate cybercrime include legitimate public measures, global regulation, and penal sanctions against cybercrime perpetrators (Adinegoro & Santiago, 2023). According to data from the Indonesian Internet Provide Association (APJI), the number of internet users in Indonesia is swiftly increasing and now exceeds 51.5% of the total population. This increase in internet users offers significant opportunities for individuals to experience the benefits of advancements in information technology. Still, it has negative consequences (such as increased cybercrimes) (Hasbullah, 2022). The criminal procedure outlined in the Indonesian Act is encouraged to address these concerns. The administrative laws of Indonesia aim to eliminate criminal offenses, such as wagering, pornography, and defamation (Marwan & Bonfigli, 2022). As countries are substantially developing legislative and administrative policies to combat the threat of cybercrime, it is important to examine Indonesia's legal frameworks for reducing cybercrimes. In addition, a small number of studies have effectively revealed the legislative policies that the Indonesian government has devised to combat cybercrime. This study explores the legal frameworks for cybercrime in Indonesian public administration to fill this gap in existing research.

This study has significant theoretical and practical implications. Regarding the academic contribution, this study investigates an important cybercrime issue concerning numerous nations. As cybercrimes become more prevalent in countries worldwide (Singh & Alshammari, 2020), examining the legal practices that can potentially combat these crimes is crucial. In addition, the number of cybercrimes in Indonesia is the second highest in the world, after Japan and individuals' awareness of the laws and hazards associated with cybercrime is extremely low (Mauladi, Laut Mertha Jaya, & Esquivias, 2022). In this regard, this study investigated the public administrative laws of Indonesia about cybercrimes, thereby substantially illuminating the perspectives of academics and researchers. In addition to advancing the theory, this study is significant for practical reasons. For instance, identifying notable regulations will enhance the knowledge of law-making authorities and policymakers to improve the implementation of cybercrime laws. Even though this

study's primary focus is Indonesia's administrative laws, this research is significant for policymakers worldwide. This research study follows a structured format to maintain paper cohesion and efficiently present pertinent data. The first section of this research focuses on the context and necessity of investigating Indonesian cybercrime laws. This section is followed by the literature review, which discusses the past literary evidence about cybercrime laws in a global context in detail. The remainder of the paper consists of the study's methodology, in which the pertinent method and its suitability for this study will be highlighted, and the study's findings, in which the law of the Indonesian legislative body about cybercrime, will be discussed. This study will conclude with a conclusion, a discussion of the study's implications, and a discussion of the study's limitations to provide an immense opportunity for future research studies.

Literature Review

Over the past decade, the increase in cybercrime issues has prompted a global evaluation of legal laws and frameworks to comprehend the development of cybercrime and its prevention. Cybercrime policing and law enforcement agencies' strong public administrative role contribute to effectively implementing legal sanctions in the cybercrime market (Collier et al., 2022). It has been observed that the legal structure or framework followed by judicial actors and local juries is effective in preventing cybercrimes and preserving safe and secure cyberspace (Al-Tawil & Younies, 2020). The General Assembly of the United Nations drafted a global cybercrime treaty in 2021, which drew the attention of law enforcement and human rights organizations to the investigation and prosecution of cybercriminals (Albader, 2022). It became necessary to conduct a scholarly assessment to examine the viability of cybercrime laws and legislation. Despite legal frameworks, the adoption of cybercrime legislation fluctuates, with Europe having the highest adoption rate and Africa having the lowest. According to Sarefo, Mphago, and Dawson (2023), the legal framework development of these two regions depends on the technology terms incorporated into the laws, making the UK cybercrime law more adaptable to the evolution and hazards of technology.

As cyber laws establish cyber security zones and hold cybercriminals accountable for misconduct, the credibility of legal frameworks is crucial to determining a country's technology environment. In the South Asian region, cyber law control bodies indicate that robust legislative functioning is the best way to minimize technology risk and threat breaches (Chang, 2020). According to the Information Technology Act of 2000 in India, cyber-attacks and offenses are evaluated, and penalties are determined (Batra et al., 2020). Even though the main act was revised in 2008 and updated to reflect the digital complexity, law enforcement agencies still use the Indian penal code from 1860 to investigate certain cybercrimes (Kumar, 2016). The UAE's federal cybercrime law body plays an important role in providing legal resolution for cyber crimes. The Federal Decree-law, IAMR policy, Electronic transaction, and trust service law, and Electronic transaction and trust service law maintain an evaluative check on digital and technological activities to reduce illegal acts in such spaces (Younies & Al-Tawil, 2020). Similarly, Bangladesh in this region has an ICT act establishing cyber tribunals and appellate courts to regulate

cybercrime activities and combat IT threats. Nonetheless, this cyber control body has certain flaws and legal issues that render it insufficient for addressing cyber security issues in this country (Babu & Ullah, 2021).

Keeping in mind the trends in cybercrime, international law enforcement agencies indicate that the lack of crime investigation tools and gaps in legal frameworks makes it difficult to stem the development of cybercrimes (Suhendi & Asmadi, 2022). Aside from the failures of legal laws and policies, the greatest obstacle is the enforcement of cyber laws. According to Ajayi (2016), the disparity between the laws and regulations of various nations is one of the greatest obstacles to implementing laws for international crimes. With the current legal frameworks, it is possible to control threats on the national level; however, digital threats on the regional level do not comply with the cyber laws on a broader scale and thus fail to provide global cyber solutions for the rising crimes. In light of the rise of the human rights movement over the past few years, the post-pandemic era poses grave digital threats. After the Europe Convention on Cybercrime, the recent United Nations cybercrime convention is a viable option for ensuring cyber security (Clough, 2023). However, the international consensus and accord may impede cyber security as a global cause. These legal setbacks result from policy proposals, which can pave the way for innovative solutions in line with the complexity of digital threats (Kleijssen & Perri, 2017).

This study focuses on the legal frameworks presently active in Indonesia for controlling and investigating cyber issues. With the increase of cyber threats in Indonesia, the ITE Law, which deals with cyberspace issues and provides a legal standard for data protection and security (Koto, 2021), governs the government's cyber regulation to defend cyberspaces. Despite the existence of a legal framework, the vulgar terminologies and legal complexities pose significant obstacles to Indonesian cyber law enforcement agencies. Machmuddin and Pratama (2017) found several vulnerabilities in Indonesian cyber law, which is problematic in light of the cyber risks in this region. Recognizing the intricacy of the Indonesian legal framework, the researcher intends to evaluate the country's cyber laws according to their administrative significance. Cyber security is viewed as a function of public administration, so the practices and procedures in this domain are crucial for cyber security management.

Methodology

This study employs qualitative methodologies to investigate the Indonesian legal frameworks regarding cybercrimes. Using a qualitative design is appropriate for this study because it comprehensively comprehends experiences, issues, and phenomena (Cleland, 2017). This study used a descriptive method to analyze data from archives, case studies, and legal framework documents in Indonesia. The data compilation method is based on primary and secondary sources. Legal documents about legislation and administrative laws constitute the primary sources, while relevant books, articles, and periodicals provide the secondary data. Jstor, the Indonesian Journal of International Law (IJIL), The Cambridge Law Journal, and the American Criminal Law Review are notable journals in this database. The data analysis in a qualitative framework employs statute analysis, in which the relevant documents are studied in-depth to extract authentic information about the phenomenon under

investigation. To reach a conclusive result, this research employs a descriptive method in conjunction with empirical judicial technique and statute analysis method. Taylor (2023) describes the method's assets as including a cost-effective and easily accessible database. In addition, the weaknesses of the methods employed in this study enable the researcher to make suggestions for future research. As the present study seeks to examine the administrative laws of cybercrime in Indonesia, recommendations were made to strengthen Indonesia's legislative structure to reduce cybercrime incidents.

Results and discussion

Cybercrime emphasizes the need for digital and cyber technology users to develop laws and regulations aimed at safeguarding the interests of every network user. Regarding cybercrime, Indonesia's legal frameworks, forms, and patterns are specified in "Law Number 11 of 2088 of chapter VII from article 27 to 37" (Sukayasa & Suryathi, 2018). The application of Cybercrime legal frameworks in Indonesia is discussed below.

Article 27: (1) Any person who, without permission or intent, transmits, distributes, or makes available any electronic data or information containing objectionable or unethical content.(2) Any person who transmits and/or distributes and/or creates electronically accessible documents or information containing a charge of wagering without the requisite rights.

(3) Any person who can distribute, communicate, or make available electronic documents or data containing derogatory and/or demeaning information.

(4) Any person who knowingly disseminates and/or distributes or makes available automatic documents or information that carries a threatening or extortion charge.

Article 28: (1) Any person with or without legal authority who disseminates incorrect, misleading, or fraudulent information in electronic communications resulting in the loss of consumers.

(2) Each individual voluntarily and illegally disseminates information intending to incite hostility or animosity toward certain individuals or community groups on the basis of race, religion, ethnicity, or intergroup.

Article 29 prohibits anyone who, without authorization or voluntarily, transmits personally-addressed electronic documents or information containing violent threats or frightening content.

Article 30: (1) Any person who intentionally, meaningfully, or illegally gains access to another individual's electronic system or computer.

(2) Any individual who intentionally or illegally gains access to a computer or electronic system to obtain electronic documents or information.

(3) A person who intentionally, unlawfully, or without authorization accesses an electronic system or a computer by breaching, heretical, breaking, or exceeding the lawfully signed security system.

Article 31: (1) A person who unlawfully, without authorization or in violation of legal procedures, interrupts electronic documents or information in any particular electronic system or computer belonging to another person.

(2) A person who illegally or voluntarily, or unlawfully intercepts electronic documents and/or electronic information that is not lawfully accessible to the public or

in a specific computer and/or "electronic system" associated with another individual, resulting in any variation or reason of any variation/alteration, termination and/or disappearance of any transmitted electronic data or electronic papers.

(3) Aside from interception described in the first and second paragraphs, interference occurs in the context of law enforcement at the request of the police, a police officer, and/or other law enforcement institutions specified by law.

(4) The interception procedure guidelines will be further governed by the specifications outlined in the third paragraph and by administration regulations.

Article 32: (1) A person who alters, adds, deletes, transfers, damages, transmits, removes, or disguises any electronic document and/or digital information associated with public property or person.

(2) A person who knowingly transmits electronic documents and/or information to an unauthorized individual or electronic system.

(3) Concerning the acts described in the first paragraph, any act that results in the disclosure of confidential digital data and/or confidential information becomes accessible to individuals with data integrity.

Article 33: Any person who unlawfully, voluntarily, or without authority causes the digitalized system to malfunction or be disrupted guilty of disturbing the electronic/digital system.

Article 34: (1) Any person who illegally, voluntarily, or unlawfully manufactures, sells, imports, disburses, delivers, or entails: a. The software or hardware of a computer designed or constructed specifically to simplify the acts described in "Articles 27 to 33"

b. Access codes, passwords of devices, or similar techniques envisioned for digital procedures to facilitate "Articles 27 to 33"-described acts.

(2) The actions described in the first paragraph are not considered illegal offenses if the intent behind the conduct is research, the digital system's examination, and the digital system's lawful protection.

Article 35: A person manipulates, produces, alerts, omits, or destroys electronic documents and/or electronic information with the intent to create electronic information and/or electronic documents that are treated as real data.

Article 36: A person who illegally, voluntarily, or against legal procedures commits or participates in an act as described in Articles 27 to 34, resulting in damage to others, shall be punished.

Article 37: A person who voluntarily engages in prohibited acts as outlined in Articles 27 through 36, excluding the "Indonesian Territory of the Electronic System in the Indonesian Juridical Territory."

Taking into account the forms and patterns of violations of "illicit action in Chapter VII," "Act Number 11/2008" also establishes the regulations for criminal activities in "Chapter XI." The implementation is briefly described below:

Article 45: (1) A person who violates "Article 27 paragraphs (1), (2), (3), and (4)" is subject to a six-year incarceration sentence and a fine of nearly "Rp 1,000,000,000.00 (one billion rupiahs)".

(2) A person who meets the criteria outlined in the first and second paragraphs of Article 28 is eligible for a six-year detention sentence and a fine of nearly one billion rupiahs.

(3) A person who meets the requirements of "Article 29" is subject to a 12-year prison sentence and a fine of "Rp 2,000,000,000.00 (two billion rupiahs)".

Article 46: (1) A person who meets the criteria outlined in Article 30's first paragraph may be sentenced to six years in prison and/or a fine of no more than "Rp 600,000,000.00 (six hundred million rupiahs)".

(2) A person who meets the criteria outlined in the second paragraph of Article 30 is subject to a maximum sentence of seven years in prison and a maximum fine of "Rp700,000,000.00 (seven hundred million rupiahs)".

(3) A person who meets the requirements of paragraph 3 of article 30 is subject to a maximum sentence of eight years in prison and/or a fine of Rp800,000,000.00 (eight hundred million rupiah).

Article 47: A person who satisfies the requirements of Article 31 paragraphs (10 and (20) is subject to a maximum sentence of "10 years" in prison and a maximum fine of "Rp8,000,000,000.00 (eight hundred million rupiah)".

Article 48: (1) Whoever fulfills the criteria outlined in Article 32 FIRST paragraph is subject to a punishment of eight years in prison and/or a fine of not more than "Rp2,000,000,000.00 (two billion rupiahs)".

(2) A person who meets the criteria of paragraph (2) of article 32 may be sentenced to a maximum of nine years in prison and a maximum fine of Rp 3 billion (three billion rupiah).

(3) A person who meets the requirements of Article 32's third paragraph is eligible for ten years of legal confinement and a maximum fine of "Rp5,000,000,000.00 (five billion rupiahs)".

Article 49 stipulates that anyone who meets the criteria outlined in Article 33 is subject to ten years in prison and a fine of "Rp10,000,000,000,000.00 (ten billion rupiahs)".

Article 50: A person who meets the requirements of Article 34 paragraph (1) is subject to ten years in detention and a maximum fine of ten billion rupiahs.

Article 51: A person who meets the criteria outlined in "Article 35" is subject to a 12-year prison sentence and an exorbitant fine of "Rp12,000,000,000.00 (twelve billion rupiahs)".

Recommendations

According to the preceding analysis, Indonesian legal frameworks regarding cybercrime are already well-established, with each article demonstrating its effective implications. In contrast, separate legal penalties and imprisonment criteria have been designed to be imposed on the person accused of cybercrime. The following recommendations can aid in preventing cybercrime and promoting the implementation of legal frameworks in light of the preceding discussion.

Despite the development of legal frameworks and articles, the number of cyberattacks in Indonesia will increase significantly between 2021 and 2022. In the first three months of 2022, the nation has received 11,8 million reports of cyberattacks. Despite severe imprisonment sentences and monetary penalties, cyberattacks are alarming to continue to plague the nation (Mauladi et al., 2022; Permana, 2021). This may be the result of inadequate implementation of legal frameworks. Therefore, the first recommendation is to strengthen the process of implementing legal measures to combat cybercrime in Indonesia. Indonesia's National Cyber and Crypto Agency must be held accountable by Indonesia's

authoritative bodies. Each individual accused of cybercrime could be subjected to the same penalties and punishments, regardless of their status or any other form of discrimination, if departments were held more accountable for their efforts to combat cybercrime.

As the incidence of cybercrime in Indonesia rises (Marliyanti, 2023; Widijowati, 2023), the Articles/legal frameworks intended to prevent cyberattacks must be revised. The conditions outlined in this framework for individuals accused of cybercrime must be tightened to increase the likelihood of being punished if convicted.

The communication divide between the Indonesian government and the National Cyber and crypto agency BSSN must be closed to increase the flow of information between the two and the likelihood of implementing adequate preventive measures for controlling the cybercrime rate in Indonesia (Rahayu, 2018). Despite Indonesia's cybercrime vulnerabilities, the government must implement comprehensive cybersecurity or data protection legislation. The Indonesian parliament introduced the UU PDP, "Undang-Undang perlindugan Data Pribadi," 2016, but the disparity between the executive and legislative branches have impeded its passage. Therefore, the government is required to evaluate its Cybercrime policies.

Conclusion

Based on the results and preceding discussion, the present research concludes that Indonesia has a sophisticated and advanced system to regulate cybercrime issues for the betterment of public administration. Data breaches negatively affect the individual whose information has been compromised and the country's reputation for lacking laws with sufficient potential to prevent cybercrime. The security intrusion results in business loss and threats to confidential documents and destroys the image of public administration policies designed to manage cybercrime. Cybercrime exerts negative influences such as carding, the existence of cracking, Twitter's piracy or other applications, cybersquatting, the usage of other accounts, leakage of data or identity theft, data imitation, extortion and sabotage, virtual port scanning, gambling, and probing, against property, against the government, and the spread of the virus in nearly every country. The implementation of the cybercrime legal framework in Indonesia includes various articles, such as "362, 363, 263, 282 and 378" statement 1 of the "criminal code, articles 56 and 29 of the UURI number 44 of 2008", Articles 303 and 8 of Law Number 7/1974, and Articles 27 to 35, 45 of Law Number 11 of 2008. Based on the occurrence of cybercrime cases in Indonesia, it is necessary to address various policies, such as updating the CPL and material criminal law, fostering security and preventive measures related to electronic devices, and provoking the establishments regarding the improvement of supervision regarding "non-penal policies" as officials' development and law enforcement officers' understanding of cybercrime (Chang, 2020). Therefore, Indonesian legal frameworks are heavily concentrated on addressing the various forms of cybercrime.

Research Implications

The present study has significant theoretical and practical implications. First, the research has contributed to the expanding corpus of literature on cybercrime. As the literature review has covered the country-by-country discussion of various

Cybercrime rules and laws, the result section has specified and narrowed the context by describing the Cybercrime legal frameworks for public administration in Indonesia. Therefore, the present research is extremely valuable because it includes information from Indonesia-specific Cybercrime articles and a general overview of cybercrime in other nations. Technology has achieved unprecedented levels of success. Therefore, it is essential to emphasize its drawbacks in the form of cybercrime, which provides hackers with simple access to the personal information of others. The most sensitive and contemporary topic has been addressed in this study, which is a worthy addition to the literature and has sound theoretical implications. The research's practical significance cannot also be denied. Indonesia's national cybersecurity departments can benefit from implementing proposed strategies to combat cybercrime in the country if they follow the recommendations in the final section of this study. The research also contributes practically because it provides an in-depth analysis of legal frameworks, which is also advantageous. Because individuals accused of cybercrime can acquire knowledge and better understand the monetary fines and imprisonment mentioned above, they may be reluctant to engage in cybercriminal activities. Governmental or authoritative entities and policymakers can also gain insight from this study to develop policies that supervise the efficient implementation of legal frameworks. Because legal acts and frameworks are not solely intended to fulfill a formality, their implementation accuracy is not the only factor of great importance.

Limitations and Future Research Indications

Despite the substantial contributions made by the study, it has some limitations. The first limitation is the geographical limitation of the study, as the administrative laws of cybercrime are examined only in the context of Indonesia. Future research can extend this topic to multiple additional nations, or a comparative study can be conducted to explore the differences between the cybercrime laws of the two countries. In addition, this study is limited by its methodological choices, as qualitative data collection was chosen. Future research could alter these methodological decisions. Future research may incorporate quantitative and mixed-method approaches to increase the generalizability of the results. In addition, this study has taken a single perspective, namely, examining Indonesia's legislative laws. In contrast, future research could broaden the topic by incorporating additional dimensions, such as the factors that increase the implementation of administrative laws to reduce the negative effects of cybercrime in Indonesia.

References

Abdulkadir, A. B., & Abdulkadir, A. O. (2019). Cybercrimes Act in Nigeria: Experimenting Compliance with Internationally Recognized Human Rights Provisions. *Journal of International Studies, 15*, 117-132. https://e-journal.uum.edu.my/index.php/jis/article/view/jis2019.15.8

Adinegoro, R., & Santiago, F. (2023). Management of Cybercrime Crimes in Indonesia Viewing from Criminal Law Political Perspective. In *Proceedings of the 2nd Multidisciplinary International Conference, MIC 2022, 12 November 2022, Semarang, Central Java, Indonesia*. EAI. http://dx.doi.org/10.4108/eai.12-11-2022.2327348

Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems, 6*(1), 1-12. https://doi.org/10.5897/JIIS2015.0089

Al-Tawil, T. N. e., & Younies, H. (2020). Corporate governance: On the crossroads of meta-regulation and social responsibility. *Journal of Financial Crime, 27*(3), 801-820. https://doi.org/10.1108/JFC-01-2020-0011

Albader, F. (2022). The pivotal role of international human rights law in defeating cybercrime: Amid a (UN-Backed) global treaty on cybercrime. *Vanderbilt Law Review, 55*, 1117. https://scholarship.law.vanderbilt.edu/vjtl/vol55/iss5/1

Babu, K.-E.-K., & Ullah, M. A. (2021). Cyber legislation and cyber-related legal issues in Bangladesh: inadequacies and challenges. *International Journal of Electronic Security and Digital Forensics, 13*(2), 180-196. https://doi.org/10.1504/IJESDF.2021.113379

Batra, S., Gupta, M., Singh, J., Srivastava, D., & Aggarwal, I. (2020). An Empirical Study of Cybercrime and Its Preventions. In *2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC)* (pp. 42-46). IEEE. https://doi.org/10.1109/PDGC50313.2020.9315785

Chang, L. Y. C. (2020). Legislative Frameworks Against Cybercrime: The Budapest Convention and Asia. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 327-343). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_6

Cleland, J. A. (2017). The qualitative orientation in medical education research. *Korean journal of medical education, 29*(2), 61-71. https://doi.org/10.3946/kjme.2017.53

Clough, J. (2023). Lessons in a Time of Pestilence: The Relevance of International Cybercrime Conventions to Controlling Post-Pandemic Cybercrime. In *Cybercrime in the Pandemic Digital Age and Beyond* (pp. 131-151). Springer. https://doi.org/10.1007/978-3-031-29107-4_7

Collier, B., Thomas, D. R., Clayton, R., Hutchings, A., & Chua, Y. T. (2022). Influence, infrastructure, and recentering cybercrime policing: evaluating emerging approaches to online law enforcement through a market for cybercrime services. *Policing and Society, 32*(1), 103-124. https://doi.org/10.1080/10439463.2021.1883608

Hasbullah, M. A. (2022). Identifying the Effects of Cybercrime on Business Laws: Implications for Businesses and Consumers. *International Journal of Cyber Criminology, 16*(2), 119-130. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/112

Khan, S., Saleh, T., Dorasamy, M., Khan, N., Leng, O. T. S., & Vergara, R. G. (2022). A systematic literature review on cybercrime legislation. *F1000Research, 11*, 971. https://f1000research.com/articles/11-971

Kleijssen, J., & Perri, P. (2017). Cybercrime, evidence and territoriality: Issues and options. In *Netherlands Yearbook of International Law 2016: The Changing Nature of Territoriality in International Law* (pp. 147-173). Springer. https://doi.org/10.1007/978-94-6265-207-1_7

Koto, I. (2021). Cyber Crime According to the ITE Law. *International Journal Reglement & Society (IJRS), 2*(2), 103-110. https://doi.org/10.55357/ijrs.v2i2.124

Kumar, P. N. V. (2016). Growing cyber crimes in India: A survey. In *2016 International Conference on Data Mining and Advanced Computing (SAPIENCE)* (pp. 246-251). IEEE. https://doi.org/10.1109/SAPIENCE.2016.7684146

Machmuddin, D. D., & Pratama, B. (2017). Some of Indonesian Cyber Law Problems. *Journal of Physics: Conference Series, 801*(1), 012089. https://doi.odi.org/10.1088/1742-6596/801/1/012089

Marliyanti, M. (2023). Optimization of Cyber Law as A Legal Basis for Handling Cyber Crime in Indonesia. *JLASA (Journal of Law and State Administration), 1*(1), 8-12. https://mubtadiinpublishing.org/index.php/JLASA/article/view/3

Marwan, A., & Bonfigli, F. (2022). Detection of Digital Law Issues and Implication for Good Governance Policy in Indonesia. *Bestuur, 10*(1), 22-32. https://doi.org/10.20961/bestuur.v10i1.59143

Mauladi, K. F., Laut Mertha Jaya, I. M., & Esquivias, M. A. (2022). Exploring the link between cashless society and cybercrime in Indonesia. *Journal of Telecommunications and the Digital Economy, 10*(3), 58-76. https://doi.org/10.18080/jtde.v10n3.533

Mittal, S., & Sharma, P. (2017). A review of international legal framework to combat cybercrime. *International Journal of Advanced Research in Computer Science, 8*(5), 1372-1374. https://dx.doi.org/10.2139/ssrn.2978744

Okutan, A. (2019). A framework for cyber crime investigation. *Procedia Computer Science, 158*, 287-294. https://doi.org/10.1016/j.procs.2019.09.054

Permana, A. (2021). Indonesia's Cyber Defense Strategy in Mitigating The Risk of Cyber Warfare Threats. *Syntax Idea, 3*(1), 1-11. https://www.jurnal.syntax-idea.co.id/index.php/syntax-idea/article/view/860

Rahayu, D. (2018). Indonesia national cybersecurity review: Before and after establishment national cyber and crypto agency (BSSN). In *2018 6th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1-6). IEEE. https://doi.org/10.1109/CITSM.2018.8674265

Sarefo, S., Mphago, B., & Dawson, M. (2023). An analysis of Botswana's cybercrime legislation. *Procedia Computer Science, 219*, 1023-1033. https://doi.org/10.1016/j.procs.2023.01.380

Singh, H., & Alshammari, T. S. (2020). An institutional theory perspective on developing a cyber security legal framework: a case of saudi arabia. *Beijing Law Review, 11*(3), 637-650. https://doi.org/10.4236/blr.2020.113039

Suhendi, D., & Asmadi, E. (2022). 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*(2), 135-143. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/35

Sukayasa, I. N., & Suryathi, W. (2018). Law Implementation of Cybercrime in Indonesia. *Soshum: Jurnal Sosial dan Humaniora, 8*(2), 123-130. https://dx.doi.org/10.31940/soshum.v8i2.985

Taylor, E. (2023). *Advantages of Secondary Research*. Ivory Research. https://www.ivoryresearch.com/library/dissertation-articles/advantages-of-secondary-research

Widijowati, D. (2023). Analysis of the Development of Cyber Crime in Indonesia. *International Journal of Artificial Intelligence Research, 6*(1.1). https://doi.org/10.29099/ijair.v6i1.1.696

Younies, H., & Al-Tawil, T. N. e. (2020). Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). *Journal of Financial Crime, 27*(4), 1089-1105. https://doi.org/10.1108/JFC-04-2020-0055