The Importance of Strengthening Legal Concepts in Overcoming Cybercrime During the Covid-19 Pandemic in Indonesia

Ardiansyah[1(✉)], M. Rafi[2], and Pahmi Amri[1]

[1] Universitas Islam Riau, Pekanbaru, Indonesia
ardiansyah@law.uir.ac.id
[2] Universitas Muhammadiyah Yogyakarta, Yogyakarta, Indonesia

Abstract. This study aims to analyze the importance of strengthening legal concepts in overcoming cybercrime during the Covid-19 pandemic in Indonesia. The Covid-19 pandemic that hit Indonesia made some people lose many things in various aspects of their lives due to multiple types of cybercrimes that often occur in society, such as malware attacks, trojan activities, and information leaks. The Electronic Information and Transactions Law (ITE) Number 11 of 2008 and the revised version of the ITE Law Number 19 of 2016 have historically been the legal basis for regulating cyber security in Indonesia. However, this regulation does not include essential parts of cybersecurity such as information and network infrastructure and human resources with cybersecurity experience. Thus, it is necessary to know how important it is to strengthen legal concepts in overcoming cybercrime during the Covid-19 pandemic in Indonesia. This study uses a qualitative approach. The data sources are from various online news media and relevant research journals and analyzed using the NVivo12 Plus application. Based on the results of the analysis, this study found that the acceleration of the ratification of the Personal Data Protection Bill, the establishment of special regulations related to cybersecurity and cybercrime, the creation of a multi-sectoral cyber security management ecosystem, as well as increasing awareness and capacity of human resources in the cyber security sector are alternative policies that must be considered and realized to strengthen the concept of law in overcoming various cyber crimes during the Covid-19 pandemic in Indonesia.

Keywords: Covid-19 pandemic · Cybercrime · Legal concepts

1 Introduction

Today, information and communication technology (ICT) has positively contributed to global economic growth and competitiveness in the public sector [1–3]. However, as government institutions, businesses, and society are increasingly connected in cyberspace, the new challenges posed by cyber threats require more attention to develop robust cybersecurity [4, 5]. Then, the existence of the Covid-19 pandemic as an unprecedented phenomenon has changed the life patterns of billions of people globally in terms of social

A. Moallem (Ed.): HCII 2022, LNCS 13333, pp. 469–479, 2022.
https://doi.org/10.1007/978-3-031-05563-8_29

norms that experience a series of circumstances related to cybercrime [6]. Where when humans experience increased anxiety due to the Covid-19 pandemic in public spaces, on the other hand, the possibility of cyber attacks also increases with a significant increase in the number [7–9].

Furthermore, after the Covid-19 pandemic in Indonesia, some people have lost many opportunities in various aspects of life due to various types of crimes that occur regularly [10]. According to data from the National Cyber and Crypto Agency (BSSN), Indonesia's number of cyber attack cases increased significantly, with 888,711,736 cyber-attacks occurring between January and August 2021, with the most common cyber-attacks being malware attacks, trojan activity attacks, and information leaks [11]. Of course, this is a problem that Indonesian law enforcement agencies must face and address to provide assurances for cybersecurity in the public arena [9, 12].

Historically, the Electronic Information and Transactions Law (ITE) Number 11 of 2008 and the revised version of the Electronic Information and Transactions Law (ITE) Number 19 of 2016 have become the legal basis for regulating cyber security in Indonesia. This legal concept regulates the distribution of prohibited content, data breaches, unauthorized access to computer systems to collect information, and illegal computer eavesdropping on other electronic systems. However, the regulation does not cover essential parts of cyber security such as information and network infrastructure and competent human resources in dealing with cybercrimes [13, 14]. In addition, law enforcement authorities' handling of cybercrime cases has not been able to be tried effectively due to non-specific regulations and the scarcity of experts to handle these cases [15]. Therefore, this research is important and exciting because the various phenomena of the many cybercrime cases during the Covid-19 pandemic in Indonesia have confused the public about the lack of specific legal frameworks in Indonesia. Thus, this study aims to answer how important it is to strengthen legal concepts in overcoming cybercrime during the Covid-19 pandemic in Indonesia.

2 Literature Review

2.1 The Phenomenon of Cybercrime During the Covid-19 Pandemic

Today, almost the entire world relies on the Internet and computer systems to manage all parts of its daily life [16]. Of course, the interconnection of the Internet and advances in technology around the world can allow criminals to abuse the potential of these networks [1, 17, 18]. Fundamentally, the Covid-19 pandemic is not just a medical problem, evidenced by the rise of cybercrime during the pandemic phase [19]. Then, various cyber crimes that continue to increase during the Covid-19 pandemic also affect digital activities to become so dominant that each individual carries out them [9, 20]. As a result, this condition continues to be exploited by cybercriminals to carry out missions that tend to harm the public sector [10, 21].

Furthermore, depending on the type of crime, the presence of the Covid-19 pandemic will impact victimization [22]. The public's tendency to engage in daily digital-based activities has increased the risk of becoming a victim of cybercrime [23]. As a result of the Covid-19 pandemic, various cybercrime phenomena have emerged, posing a considerable threat to people's safety and the global economy around the world [24].

Thus, Cybercrime phenomena during a pandemic must be analyzed to find fundamental principles for overcoming and responding to current and future cybercrime events [25].

2.2 Legal Concepts in Cybercrime

Cybercrime is conceptually an act of crime committed through ICT and is a significant threat today. The threat is not only to individuals but also to government organizations and businesses [26]. Cybercrime is still a new phenomenon because criminals no longer need to be close to their victims but can attack and steal from a distance [27]. The impact of cybercrime causes financial and intangible losses. It even impacts the risk of global peace and security [28]. In particular, the first provision as an international response is the cybercrime legal convention. The substance of the Cybercrime Convention includes material criminal law, procedural law, business accountability, and international cooperation [29]. Currently, Indonesia's position in regulation has not ratified the international cybercrime legal convention. However, only adopting cybercrime legal conventions are substantially broader and not specific in Law Number 11 of 2008 concerning Information and Electronic Transactions and Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions [30].

In the process, the weak concept of law enforcement is a factor causing the increase in cybercrime cases that occur [31]. So, security policies in legal products must be improved to deal with all types of questionable cybercrime activities [32]. Then, strengthening the concept of cybercrime law must be carried out effectively in advances in technology and information [33, 34]. In addition, in times of disturbance and uncertainty, each future regulatory actor should also be involved in a more recursive and reflective analysis to increase responsiveness [35]. Therefore, several research reviews have concluded that strengthening the concept of cybercrime law should be a top priority for all governments [36].

3 Research Methods

This study uses a qualitative approach to analyze various phenomena from secondary data, including government websites, books, journals, proceedings, and national online news media content such as tribunnews.com, kompas.com, and detik.com. Then, data collection techniques will focus on various legal concept literature and cybercrime phenomena during the Covid-19 pandemic in Indonesia's national online media. The Nvivo 12 Plus application performed crosstab analysis on the qualitative data [37, 38]. Furthermore, there are five stages in using Nvivo 12 Plus: data collection, data entry, data coding, data classification, and data display. The processed data through Nvivo will then proceed to visualize the qualitative analysis.

4 Result and Discussions

In Indonesia, various cybercrime incidents have always been a trending issue in the public space since the onset of the Covid-19 pandemic on March 2, 2020-December 23,

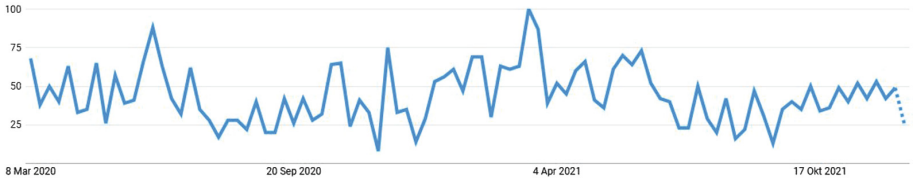

Fig. 1. Trends in cybercrime issues during the Covid-19 pandemic in Indonesia. Source: [39]

2021. The trend in question is the threat of cybercrime that can harm the public sector (Fig. 1).

Then, in the process, various cybercrime phenomena are growing over time. During the covid-19 pandemic, it has emphasized and visualized that Indonesia needs to strengthen legal concepts to minimize the occurrence of cybercrime, which is increasingly happening in public spaces.

4.1 The Phenomenon of Cybercrime During the Covid-19 Pandemic in Indonesia

Currently, various countries face cybercrime phenomena amid the Covid-19 pandemic, which has also changed the global cyber threat landscape. Hackers take advantage of the desire for information and online transactions to launch attacks and gain illegal profits in an all-digital culture. Cybercriminals target billions of vigilant people and have a crucial role in reacting to the pandemic, such as governments and other relevant organizations, without regard to ethics. Cybercriminals also use network security weaknesses to attack companies whose employees must work from home due to the Covid-19 pandemic [10]. Then based on data processing through the Nvivo 12 Plus software on the specified online media, there are several types of cybercrime attacks during the Covid-19 pandemic in Indonesia, namely:

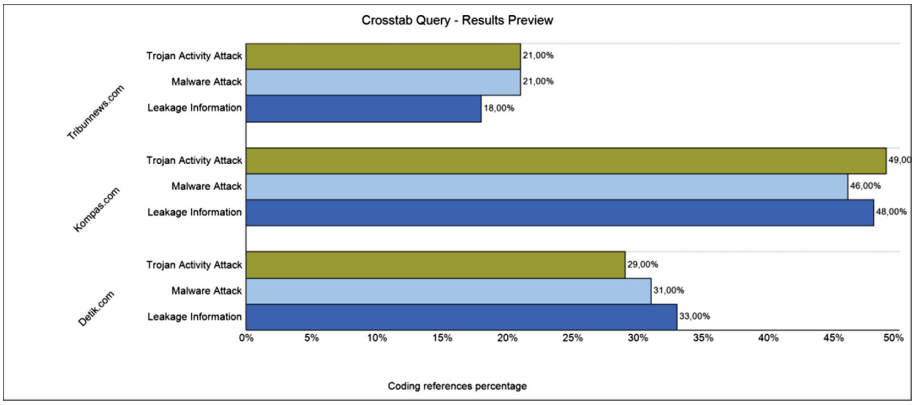

Fig. 2. Crosstab analysis on cyber crime attacks during the Covid-19 pandemic in Indonesia

Figure 2 shows that during the Covid-19 pandemic in Indonesia, there were numerous assaults, including trojan-activity attacks, malware attacks, and information leaking. Then, the most dominant online media in highlighting the issue of trojan-activity attacks is kompas.com (49.18%), followed by detik.com (29.51%) and tribunnews.com (21.31%). Malicious software that can harm a system or network is a Trojan activity attack. Trojans are not detectable like viruses and worms. However, they are challenging to discover since they often look like common apps or files, such as mp3 files, free software, phony antivirus, and free games. There are various types of Trojan malware, namely AllAple, ZeroAccess, WillExec, Glpteba, and CobaltStrike. The purpose of a trojan-activity attack is to steal information from the victim, such as passwords, log data, credentials, and other sensitive information. Trojan exploits pose a severe threat to victims if hackers gain access to the system and gain access to sensitive data. As a result, based on monitoring data from the Indonesian National Cyber Security Operations Center throughout 2020, Trojans became the anomaly with the highest number [40].

Furthermore, kompas.com (48.33%) is the most dominating online media in highlighting information leakage, followed by detik.com (33.33%) and tribunnews.com (18.34%). Another cyber-attack has happened, this time involving a data breach at the Health Social Security Administering Body (BPJS). Due to hacking, information belonging to 279 million Indonesians was stolen and sold on internet forums (dark web). The information transferred includes full name, PIN, date of birth, email, and mobile number. The information is then traded for 0.15 bitcoin, equivalent to 81.6 million Indonesian rupiahs [41]. The phenomenon of data leakage is certainly hazardous because vulnerable to abuse for various cybercrimes, such as bank account hijacking and fake online loans.

In the aspect of malware attacks, the most dominant online media highlighting this type of attack is kompas.com (46.67%), followed by detik.com (31.61%) and tribunnews.com (21.66%). The type of malware attack in question has long been a broad multidirectional attack because cybercriminals will exploit information systems using software containing viruses, trojans, worms, or ransomware. Malware attacks that encrypt files and demand ransom and Distributed Denial of Service (DDoS) are two types of cyber attacks that are increasing and worrying [42]. Then, most malware attacks have common targets that can harm a more comprehensive system. As a result, individual cybersecurity knowledge and assistance from authority figures in the pandemic era are critical to building a safe environment in remote work [10]. Several cybercrime attacks in Indonesia during the COVID-19 pandemic exposed the vulnerability of the Indonesian state to digital security systems due to the lack of adequate protective measures and particular legal concepts.

4.2 The Importance of Strengthening Legal Concepts in Overcoming Cybercrime During the Covid-19 Pandemic in Indonesia

Currently, the Information and Electronic Transactions (ITE) Law Number 11 of 2008 and Law Number 19 of 2016 are the legal basis for regulating cyber security in Indonesia. The ITE law prohibits various offenses, including distributing prohibited content, breaches of data protection, unauthorized access to other computer systems to collect

information, and unauthorized interception of computer systems or other electronic systems. Substantially, the ITE Law protects the contents of electronic systems and electronic transactions legally. However, the ITE Law does not address critical cybersecurity areas such as information and network infrastructure and human resources [5].

Based on the 2016 ITE Law, the Government stipulates technical regulations in Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. As stated in Government Regulation Number 71 of 2019, updating cyber security in electronic systems and transactions has set more stringent laws for personal data and information security and website authentication to avoid fake and fraudulent sites. Furthermore, Government Regulation No. 71 of 2019 emphasizes the importance of developing a national cybersecurity plan to prevent harm to the public interest caused by misuse of information and electronic transactions such as data misuse, illegal electronic signatures, and the spread of viruses and malicious codes. However, the ITE Law and Government Regulation Number 71 of 2019 do not provide adequate protection for ever-changing cyber threats, especially those affecting critical infrastructure in the government sector.

After that, the Minister of Defense Regulation No. 82 of 2014 provides cyber defense principles to deal with cyber threats to national security. This rule then de-fines cyber security, referring to all government actions to protect information and technology. This regulation explains that cyber-attacks are every statement or action of any party that damages national security, sovereignty, and territorial integrity. Unlike the ITE Law, this regulation includes critical infrastructure as cybersecurity objects, such as financial and transportation networks. However, this regulation only enhances the military's cyber defense capabilities created and implemented for the Indonesian National Armed Forces (TNI). For non-military cyber threats, only refer to the regulations in the ITE Law.

In the process, the rules and regulations of cyber security in Indonesia resulted in the division of tasks between several ministries. Of course, this becomes ineffective in preventing cybercrime. As a result, specific cyber security regulations have become very important for state security in Indonesia. The following is a design for strengthening the legal concept in overcoming cybercrime during the Covid-19 pandemic in Indonesia (Table 1).

Table 1 illustrates that perfecting legal concepts is very important to overcome cybercrime during the covid-19 pandemic in Indonesia. Alternative policies can be implemented by: First, accelerating the ratification of the Personal Data Protection Bill. Second, pass specific laws related to cybersecurity and cybercrime. Third, create a cybersecurity ecology. Furthermore, Fourth, to increase the capacity of human resources.

5 Conclusions

Various cybercrime attacks throughout the pandemic have shown that Indonesia still does not have an adequate protection system, and the legal concept is not yet specific. This study concludes that the draft for strengthening the legal concept can start by accelerating the ratification of the Personal Data Protection Bill. Then, pass special laws related to cyber security and cybercrime. Furthermore, create a cybersecurity ecology. The last

Table 1. Design of strengthening legal concepts in overcoming cybercrime attacks during the Covid-19 pandemic in Indonesia. Source: [43].

Number	Policy alternative	Legal concept design
1	Accelerate the passage of the Personal Data Protection Bill	Based on the availability of security policy documents, legal certainty in cyber security can regulate all information security procedures. Therefore, the discussion of the Personal Data Protection Bill must be realized immediately and maintain an anticipatory premise in the increasingly rapid development of technology. Then, the Personal Data Protection Bill must also be based on various government actors, the private sector, and the people's consultative council (DPR-RI). It aims to unify all existing regulations to be more integrated into all types of personal data, data owner rights, data processing, data controllers, data transfer, dispute resolution, and the imposition of administrative and criminal sanctions
2	Establish special regulations dealing with cyber-security and cyber-crime	The complexity of the threat of cyber attacks in the public, government, and private sectors necessitates the development of two regulatory products that tightly regulate domestic and worldwide cyber security and cybercrime. Cybersecurity legislation should address the concerns of protecting critical infrastructure from cyberattacks and cross-sectoral coordination. In addition, Indonesia needs an autonomous institution to foster cross-sectoral cooperation in handling cyber cases in the public, private, and government sectors. Strict rules must emphasize the phenomenon of cybercrime in behavioral problems and types of cybercrime as well as steps to combat it on a national and global scale

(*continued*)

Table 1. (*continued*)

Number	Policy alternative	Legal concept design
3	Creation of a multisectoral cybersecurity management ecosystem	Cybercrime threats are increasingly complex and widespread in various sectors in the pandemic era, requiring optimal coordination and synergy between various stakeholders. The stakeholders in question are the National Cyber and Crypto Agency, Cybercrime Police, the Ministry of Communication and Information, and the State Intelligence Agency. The sectoral ego that is still happening so far has made cyber handling in Indonesia stagnating, so sweeping changes must be made. Then, the Government of Indonesia can also build cross-sectoral ecosystem collaboration by following the approach used in the UK and other European countries by involving independent non-profit organizations
4	Increase awareness and capacity of human resources in the field of cyber security	During the Covid-19 pandemic in Indonesia, various government organizations must immediately organize online webinars in various media to educate the public about various types of cybercrime attacks. The organizations in question are the Ministry of Communication and Information, the National Cyber and Crypto Agency, the Financial Services Authority, and Bank Indonesia. Then, the National Cyber and Crypto Agency must also provide support to various companies throughout the Indonesian industry to improve the security of information systems and networks. In addition, the Government must also address the issue of human resource capabilities, especially for the younger generation to be directly involved in career paths and training in cyber security

step increases the capacity of human resources. The limitation of this study is that it only uses data from online news sources and focuses on analyzing the phenomena and significance of increasing the concept of cybercrime law during the pandemic. Therefore, we recommend that further research be conducted on the Penta helix to strengthen the concept of cybercrime law in Indonesia.

References

1. Thomas, A.M.B., Holt, J.: The Palgrave Handbook of International Cybercrime and Cyberdeviance. Springer, Switzerland (2020). https://doi.org/10.1007/978-3-319-78440-3
2. Shalaginov, A., Shalaginova, M., Jevremovic, A., Krstic, M.: Modern cybercrime investigation: technological advancement of smart devices and legal aspects of corresponding digital transformation. In: IEEE International Conference on Big Data, Big Data, pp. 2328–2332 (2020). https://doi.org/10.1109/BigData50022.2020.9378224
3. Koto, I.: Cyber crime according to the ITE law. Int. J. Reglem. Soc. **2**(2), pp. 103–110 (2021). http://jurnal.bundamediagrup.co.id/index.php/ijrs/article/view/124
4. Djanggih, H., Thalib, H., Baharuddin, H., Qamar, N., Ahmar, A.S.: The effectiveness of law enforcement on child protection for cybercrime victims in Indonesia. J. Phys. Conf. Ser. **1028**(1), 1–8 (2018). https://doi.org/10.1088/1742-6596/1028/1/012192
5. Anjani, N.H.: Cybersecurity protection in Indonesia. Cent. Indones. Policy Stud. **1**(9), 1–12 (2021). https://www.cips-indonesia.org/post/policy-brief-cybersecurity-protection-in-indonesia
6. Buil-Gil, D., Zeng, Y., Kemp, S.: Offline crime bounces back to pre-COVID levels, cyber stays high: interrupted time-series analysis in Northern Ireland. Crime Sci. **10**(1), 1–16 (2021). https://doi.org/10.1186/s40163-021-00162-9
7. Umanailo, M.C.B., et al.: Cybercrime case as impact development of communication technology that troubling society. Int. J. Sci. Technol. Res. **8**(9), 1224–1228 (2019). https://doi.org/10.5281/zenodo.3457420
8. Wijaya, M.R., Arifin, R.: Cyber crime in international legal instrument: how Indonesia and international deal with this crime? IJCLS (Indonesian J. Crim. Law Stud. **5**(1), pp. 63–74 (2020). https://doi.org/10.15294/ijcls.v5i1.23273
9. Lallie, H.S.: Cyber security in the age of Covid-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Comput. Secur. **105**, 102248 (2021). https://doi.org/10.1016/j.cose.2021.102248
10. Amarullah, A.H., Runturambi, A.J.S., Widiawan, B.: Analyzing cyber crimes during Covid-19 time in Indonesia. In: 3rd International Conference on Computer Communication and the Internet (ICCCI), pp. 78–83 (2021). https://doi.org/10.1109/ICCCI51764.2021.9486775
11. Cnnindonesia.com, BSSN: Ada 888 Juta Serangan Siber Sepanjang 2021 (2021). https://www.cnnindonesia.com/nasional/20210913131225-12-693494/bssn-ada-888-juta-serangan-siber-sepanjang-2021. Accessed 20 Dec 2021
12. Rachh, A.: A study of future opportunities and challenges in digital healthcare sector: Cyber security vs crimes in digital healthcare sector. Asia Pacific J. Heal. Manag. **16**(3), 7–15 (2021). https://doi.org/10.24083/apjhm.v16i3.957
13. Makarim, E.: Privacy and personal data protection in indonesia: the hybrid paradigm of the subjective and objective approach. In: Kiesow Cortez, E. (ed.) Data Protection Around the World. ITLS, vol. 33, pp. 127–164. T.M.C. Asser Press, The Hague (2021). https://doi.org/10.1007/978-94-6265-407-5_6
14. Hicks, J.: A 'data realm' for the Global South? Evidence from Indonesia. Third World Q. **42**(7), 1417–1435 (2021). https://doi.org/10.1080/01436597.2021.1901570

15. Cortez, E.K.: Data Protection Around the World: Privacy Laws in Action, 3rd edn. Asser Press, The Hague (2021). https://www.asser.nl/asserpress/books/?rId=13963
16. Paat, Y.F.: Digital crime, trauma, and abuse: Internet safety and cyber risks for adolescents and emerging adults in the 21st century. Soc. Work Ment. Health **19**(1), 18–40 (2021). https://doi.org/10.1080/15332985.2020.1845281
17. Perrone, G.: Online crimes as a result of a digital interconnection system. A cyber criminological reflection. Rass. Ital. di Criminol. **15**(3), 239–247 (2021). https://doi.org/10.7347/RIC-032021-p239
18. Miguel, C.S.: Online victimization, social media utilization, and cyber crime prevention measures. Asia-Pacific Soc. Sci. Rev. **20**(4), 123–135 (2020). https://www.scopus.com/inward/record.uri?partnerID=HzOxMe3b&scp=85097731756&origin=inward
19. Gryszczyńska, A.: The impact of the Covid-19 pandemic on cybercrime. Bull. Polish Acad. Sci. Tech. Sci. **69**(4), 1–9 (2021). https://doi.org/10.24425/bpasts.2021.137933
20. Olofinbiyi, S.A.: The role and place of covid-19: an opportunistic avenue for exponential world's upsurge in cyber crime. Int. J. Criminol. Sociol. **9**, 221–230 (2020). https://doi.org/10.6000/1929-4409.2020.09.20
21. Boussi, G.O.: A proposed framework for controlling cyber- crime. In: ICRITO 2020 - IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), pp. 1060–1063 (2020). https://doi.org/10.1109/ICRITO48877.2020.9197975
22. Hawdon, J., Parti, K., Dearden, T.E.: Cybercrime in America amid COVID-19: the initial results from a natural experiment. Am. J. Crim. Justice **45**(4), 546–562 (2020). https://doi.org/10.1007/s12103-020-09534-4
23. Akdemir, N.: Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: a lifestyle routine activities approach. Internet Res. **30**(6), 1665–1687 (2020). https://doi.org/10.1108/INTR-10-2019-0400
24. Díaz, R.M.: Cybersecurity in the time of Covid-19 and the transition to cyberimmunity. FAL Bulletin 382: Economic Commission for Latin America and the Caribbean (ECLAC), no. 6, Latin America and the Caribbean, pp. 1–17 (2020). https://www.cepal.org/en/publications/46511-cybersecurity-time-covid-19-and-transition-cyberimmunity
25. Vienna: Cybercrime and Covid-19: Risks and Responses. United Nations Office on Drugs and Crime, Wina (2020). https://www.unodc.org/documents/Advocacy-Section/UNODC_-_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf
26. Cordova, J.G.L., Álvarez, P.F.C., De Jesús Echerri Ferrandiz, F., Pérez-Bravo, J.C.: Law versus cybercrime. Glob. Jurist **18**(1), 1–9 (2018). https://doi.org/10.1515/gj-2017-0024
27. John Bandler, A.M.: Cybercrime Investigations: A Comprehensive Resource for Everyone, 1st edn. CRC Press, New York (2020). https://doi.org/10.1201/9781003033523
28. Christou, G.: The challenges of cybercrime governance in the European Union. Eur. Polit. Soc. **19**(3), 355–375 (2018). https://doi.org/10.1080/23745118.2018.1430722
29. Maillart, J.-B.: The limits of subjective territorial jurisdiction in the context of cybercrime. ERA Forum **19**(3), 375–390 (2018). https://doi.org/10.1007/s12027-018-0527-2
30. Bunga, D.: Legal response to cybercrime in global and national dimensions. Padjadjaran Jurnal Ilmu Hukum (J. Law) **06**(01), 69–89 (2019). https://doi.org/10.22304/pjih.v6n1.a4
31. Zharova, A., Elin, V.: On the using datamessage as evidence of cybercrime. IOP Conf. Ser. Mater. Sci. Eng. **1069**(1), 012037 (2021). https://doi.org/10.1088/1757-899x/1069/1/012037
32. Shalaginov, A.: Big data analytics and artificial intelligence for cyber crime investigation and prevention. Futur. Gener. Comput. Syst. **109**, 702–703 (2020). https://doi.org/10.1016/j.future.2020.04.007
33. Maskun: Qualifying cyber crime as a crime of aggression in international law. J. East Asia Int. Law, **13**(2), 397–418 (2020). https://doi.org/10.14330/jeail.2020.13.2.08

34. Sikos, L.F.: AI in digital forensics: ontology engineering for cybercrime investigations. WIREs Forensic Sci. **3**(3), 1–11 (2021). https://doi.org/10.1002/wfs2.1394
35. Walker-Munro, B.: A case for the use of cyber-systemics to combat financial crime in Australia. Kybernetes **50**(11), 3082–3105 (2021). https://doi.org/10.1108/K-09-2020-0581
36. Koziarski, J., Lee, J.R.: Connecting evidence-based policing and cybercrime. Polic. An Int. J. **43**(1), 198–211 (2020). https://doi.org/10.1108/PIJPSM-07-2019-0107
37. Hai-Jew, S.: "NVivo 12 plus's new qualitative cross-tab analysis function. Kansas State University (2020). https://scalar.usc.edu/works/c2c-digital-magazine-fall-2018--winter-2019/nvivo-12-plus-new-qual-cross-tab-analysis-function
38. Sotiriadou, P., Brouwers, J., Le, T.: Choosing a qualitative data analysis tool: a comparison of NVivo and Leximancer. Ann. Leis. Res. **17**(2), 218–234 (2014). https://doi.org/10.1080/11745398.2014.902292
39. Google.com: Trends in cyber crime issues during the Covid-19 pandemic in Indonesia (2021). https://trends.google.com/trends/explore?date=2020-03-022021-12-23&geo=ID&q=CyberCrime. Accessed 23 Dec 2021
40. Tribunnews.com, BSSN: Ada Tren Peningkatan Serangan Siber Malware Pencuri Informasi di Awal Pandemi (2021). https://www.tribunnews.com/nasional/2021/03/01/bssn-ada-tren-peningkatan-serangan-siber-malware-pencuri-informasi-di-awal-pandemi?page=3. Accessed 24 Dec 2021
41. Kompas.com, Kronologi Kasus Kebocoran Data WNI, Dijual 0,15 Bitcoin hingga Pemanggilan Direksi BPJS (2021). https://tekno.kompas.com/read/2021/05/22/09450057/kronologi-kasus-kebocoran-data-wni-dijual-0-15-bitcoin-hingga-pemanggilan?page=all. Accessed 24 Dec 2021
42. Detik.com, BSSN dan BPS Kerja Sama Perkuat Keamanan Data dari Serangan Siber, (2021). https://inet.detik.com/security/d-5767571/bssn-dan-bps-kerja-sama-perkuat-keamanan-data-dari-serangan-siber?_ga=2.51210796.46083478.1640343522-756276621.1635146417. Accessed 25 Dec 2021
43. Wicaksana, R.H., Munandar, A.I., Samputra, P.L.: A narrative policy framework analysis of data privacy policy: a case of cyber attacks during the Covid-19 pandemic. J. Ilmu Pengetah. dan Teknol. Komun. **22**(2), 143–158 (2020). https://doi.org/10.33164/iptekkom.22.2.2020.143-158