Examining the Adequacy of Constitutional Laws Related to Cybercrimes in Indonesia

Imam Mahdi[1]
Universitas Islam Negeri Fatmawati Sukarno, Indonesia

Juhriyansyah Dalle[2]
Universitas Lambung Mangkurat, Indonesia

Abstract

Without a comprehensive cybercrime law, it is difficult for any country to prevent cybercrimes. Cybercrimes are committed using Internet and information technology related tools. This paper highlights how a few constructs such as conventional views of cybercrime; information about the types of cybercrime available at community level; role of the cyber police and use of information technology for its investigation can assist in framing constitutional laws to prevent cybercrimes in Indonesia. In a qualitative framework, using document survey as the research tool, this study describes how the constitutional law should control and guide the transmission of the conventional view about cybercrimes at the community level. It also suggests measures to interpret and assist in the investigation of any problems and inequalities, with the help of cyber police and information technology aids. The results and findings reveal that the current Indonesian laws related to prevention of cybercrimes are inadequate and require over-hauling. There is a need to judge how cyber criminals execute crimes and prepare legal clauses and provisions accordingly to curb them. The study findings will be a good source of reference for lawmakers and other experts who could be benefited with the recommendations of this study

Keywords: cybercrime laws, cyber police, information technology, Indonesia

Introduction

Cybercrime is termed as a criminal offence involving a computer or a computer network with the primary motive to make money illegally, and often committed for political or personal reasons. Cybercriminals or hackers are highly technically skilled individuals or organizations that make use of advanced techniques, often difficult to anticipate even by cyber criminologist. They can access the user's personal information, their classified business data, and end with disabling a device. Such cybercriminals are indulged in selling online such illicit information. Cyber Criminology is although a multidisciplinary subject, which

[1] Faculty of Syariah, Universitas Islam Negeri Fatmawati Sukarno, Bengkulu 38211, Indonesia. E-mail: imam.mahdi@iainbengkulu.ac.id
[2] Department of Information Technology, Universitas Lambung Mangkurat, Banjarmasin 70123, Indonesia. E-mail: j.dalle@ulm.ac.id

involves disciplines like Criminology, Victimology, Sociology, Internet Science, and Computer Science, it keeps evolving with the state of art technology. Jaishankar (2007) defined Cyber Criminology as "the study of causation of crimes that occur in the cyberspace and its impact in the physical space". It is a body of knowledge that though deals with cybercrimes but not engaged in any crime investigation or cyber forensics. For the purpose of investigation, a separate discipline is required which can independently examine the cybercrimes from social as well as legal perspective. Despite rigorous attempts by law enforcement agencies and constitutional provisions, the issue of cybercrimes continues to grow. It costs companies and individuals billions of dollars annually with no end in sight (Brewer et al., 2018; Ketaren, 2016).

Cybercrimes generally fall into two categories: first, crimes that target networks or users' devices through viruses, malware DoS attacks and botnets; second, crimes that use hacking devices to commit cybercrimes such as phishing, Website spoofing, cyberstalking, identity theft and Intellectual Property Theft. (Ismail, 2009; Juditha, 2016). A virus is a program that is designed to attack users' devices– computers, tablets, smartphones and other digital devices. It gains access to the user's device, steals all the personal data and might crash, reboot or slow down the device. It can also slow down their internet connection as it searches for other devices to infect or access their data too. A virus is one kind of malware: other kinds include worms such as Trojans and spywares. Worms spread from one device to another; they can multiply hundreds of times. A Trojan horse is a deceptive malware that pretends to be safe and useful but actually attack the user's device. A spyware is software that installs itself onto devices and steals personal information of the user like passwords and email addresses and even the webcam without the user's knowledge. A modern–day type of malware is ransomware designed for extortion. A cybercriminal steals a thing of great value or keeps a huge amount of data as hostage from the user's device and demands payment in exchange for its return. In businesses, when a ransomware hits, employees cannot do their jobs unless the lost data is restored. DoS attacks are mostly seen in networks where an online service is made unavailable by the attacker. The hacker overwhelms a website with traffic from other networks and infect malwares known as Botnets in the user's computer. Once the network is done, the remote hacker gains the access to the system and steals the information.

Phishing occurs when cybercriminals send fraudulent emails pretending to be from the user's contacts or from legitimate websites. The attacker sends phishing emails and tricks people to share personal information or click a malicious link in order to gain access to their devices. Website spoofing aims at deceiving a user through a website that looks like the real one. The website spoofer replicates a website with the same brand, style, logo and even domain name thus tricking the user to give access to passwords and personal data. Cyberstalking is a kind on online harassment through a plethora of online messages and emails. The cyberstalked exploits the social media accounts and search engines to identify susceptible users. They create situation of fear, anxiety and insecurity in the victim.

A cybercrime is committed to steal user's identity. The identity theft, as it is called, takes place when the attacker secures the user's identity through his credentials and steals funds, accessed confidential information, or commit tax, baking or insurance frauds. Intellectual Property Theft, commonly known as piracy, is committed by illegally obtaining books, music albums, movies, and making them available for free download. Such illegal downloads might also contain hidden malware to destroy your computer. Locally, in the user's device, there are also a few other malwares that can take place without the user's knowledge. For instance, a key logger or keystroke logger is a program that records the characters typed by

the user. The perpetrator installs the key logger program on a public computer and traps all the characters pressed by the user with the hope to get user ID and password of the victims. A similar attempt can be made by a perpetrator to steal a user's ID and password by a program called 'Sniffing'. This program sniffs or chases data packets passing over a computer network. Likewise, there are programs such as Brute Force, capable of stealing a user's password by trying all possible combination; Web Deface which is capable of changing the appearance of a website or its home page; Disabling Service, by flooding large amount of data with the intention of disabling the system; last but not the least, emails spams, worms, and Trojans, which are most commonly deployed by hackers to breach into the system (Tianotak, 2011).

Owing to these multiple types of cybercrimes and malware programs, cyber-criminology becomes an exciting frontier for legal experts in criminology. Although there exist several constitutional provisions and cyber laws to prevent these crimes, the virtual nature of these crimes and internet mediated communications poses greater challenge to the law makers. The cybercriminals act beyond the traditional discourse of criminology, with innovative forms of crime and deception, thus giving shape to a new locus of criminal activity (Loader & Thomas, 2013; Putra, 2014; Rondelez, 2018; Yar, 2005).

An electronic contract is defined as an agreement made through an electronic system. Hence, online transactions are recognized as electronic transaction under this agreement. Prior to every transaction, there precedes an acceptance of the terms and conditions of the online transaction. While filing the electronic contract, the applicant provides personal information such as the identities of the parties, their other specifications like account numbers, zip codes and so on. The challenge before the data collection agency, which may be a bank, an insurance company, a financial vendor, a money exchanger, or a payment portal, is data protection and privacy. In the case of any absence of a comprehensive cyber law, such regulations may have to take place with specific rules related to such data packets provided in electronic contracts.

This study aimed to examine the constitutional laws related to Cyber criminology in Indonesia. The Indonesian government has failed to take significant steps to prevent cybercrime and preferred to use only the conventional laws (Ismail, 2009; Sari et al., 2018) such as Indonesian Criminal Code, 19 and the Electronic Information and Transactions Law, 20; which are used only to frame a few subsidiary acts and legislations concerning cybercrimes. These acts and legislations are very broad in nature and cover a wide scope of crimes related to consumer protection, data protection, intellectual property, e-commerce, electronic contracts, but less concerning severe types of cybercrimes like cybersquatting (domain name related case). However, in 2017, the Indonesian Government established the National Cyber and Crypto Agency, an agency to control cybercrime and to offer cyber defense to victims against all malware, spams, phishing and hacking threats (Daryono & Sugiantoro, 2017). In spite of these initiatives, Arifah (2011) laments that Indonesia's legal framework on cybercrime and cybersecurity deals only with specific incidents and when only they take place. In addition, these legal frameworks carry a very conventional view of cybercrime.

This paper is divided into five sections: The first section discussed the background, meaning and purpose of cyber criminology in the Indonesian context. It also included various types of cybercrimes and showed how the constitutional law took only conventional approach to combat these crimes, where there is a dire need to curb this evil. The second section reviews the legal and regulatory measures and the Indonesian legal framework that currently exists in Indonesia to prevent cybercrimes. It also shows how the use of

Information technology can prevent cybercrimes and what role can cyber police play to assist in the investigation of these crimes. The third section presents the theoretical framework and research methodology used in this study. The fourth section summarizes all the available data in various legal and research documents related to cybercrimes and their preventions. Finally, there is a conclusion with perspectives on cybercrimes and recommendations for their prevention.

Literature Review

Constitutional; Law in Indonesia

Indonesia currently lacks a comprehensive data protection law, however, there are a few sectoral laws that govern data privacy. For instance, the Electronic Information and Transactions Law, 19 allows every Indonesian citizen the right to request the service provider to delete and permanently forget the electronic information or documents from their electronic records system (Fahlevi et al., 2019). In case of a breach of this regulation and if any individual suffers any loss, theft or cyber-attack, the victim can submit complaints to the Minister of Communications and Information, Indonesia to intervene and ensure the protection and confidentiality of their personal data.

The provision of UU No.36 of 1999 majorly focused on telecommunication and the rights of the individual users. This Law on Telecommunications,1999 mandated the service providers to keep users' data confidential across all telecommunications networks. It also required the service provider to provide users security and privacy. For government accounts, the service providers were required to provide extra security as it held classified information over its network. In 2003, for the first time, the Indonesian Information and Communication Ministry (Kemenkominfo) formulated a law to defend against cybercrime. Five years later, in 2008, Indonesian President Susilo Bambang Yudhoyono signed the UU-ITE (Information and Electronic Law) and named it "Undang-Undang Nomor 11 tahun 2008". This was followed with other cyber laws namely UU KPI (Public information openness law) 14/2008 and UUP (Pornography law) 44/2008. These laws streamlined the online content regulations and provided privacy and safety to the users. As a result, Indonesia's e-commerce prospered as both individuals and business entities had the privilege of legal assurance. They knew that their personal and business transactions done electronically through the Internet were safe and protected against any malware, phishing, cyberstalking or identity theft.

The Indonesian legal system has laid down provisions for crimes like defamation, hacking, breach of copyrights and trademarks, that were also directly or indirectly brought in the jurisdiction of cybercrimes (Dmello & Bichler, 2020; Hegazy, 2021; Nasrollahzadeh & Koramaz, 2020; Yar, 2005; Yasutomi, 2020). Defamation through the Internet under the cyber-law, for instance, was regulated under Article 310 of the Criminal Code of Indonesia and the Electronic Information and Transactions Law. The Law made defamation a punishable offence, where the offender may be sentenced up to six years of imprisonment and a fine of up to IDR 1 billion. Similarly, the Law also recognized Identity fraud as an unlawful misrepresentation when done by manipulating the user's personal data and was punishable by a maximum imprisonment of 12 years and/or a fine of IDR 12 billion. Broadening the scope of this Law, it laid down the provision that any unlawful transfer of electronic information or electronic records through breaching, hacking, trespassing, or breaking through a security system was punishable by a maximum imprisonment of eight years and/or a maximum fine of IDR 800 million.

Intellectual Property (IP) Laws are also linked with the cyber laws and covered regulations on copyright, trademarks, patents, and trade secrets. It was an important step to include IP Laws as a part of cyber laws. With this inclusion of IP rights under the cyber law, other Indonesian laws related to IP were also revised and reviewed. For instance, Copyright Law No. 28 of 2014 replaced the previous Copyright Law No. 19 of 2002. Special provisions governing copyrighted content and related rights in information and communication technology were added in the amended law. Regulations were laid out for the production, storage, distribution and viewing of information technology devices which included optical discs, servers, cloud computing, secret codes, passwords, barcodes, serial numbers, technology descriptions, and encryption. The IP rights also protected copyright infringement and rights related to information technology-based facilities. Likewise, there are laws related to Trademarks-- Law No. 20 of 2016, which comprises checks trademark infringements and imposes punishments for counterfeits; Patents -- The Patents Law No. 13 of 2016, which protects the exclusive rights of the patent holder provided the patent is registered with the Directorate General of Intellectual Property; Trade Secret-- Trade Secret Law No. 30 of 2000, which checks infringement of trade secrets with the intention to breach a contract.

Conventional view vs community awareness about cyber crimes

The currently applicable laws in Indonesia are mostly related to conventional view of cybercrimes, such as crimes committed by making use of computers or internet or those related to intellectual property rights. Although these laws have developed a lot of public and community awareness for cybercrimes, but the problem faced is in the legal process that takes place after a crime is committed. The current laws have failed to pace up with the variety and multiplicity in the nature of cybercrimes. The process of investigation of new types of cybercrimes is same as the conventional criminal cases, where the violators breached the basic laws of the internet or committed crimes like hacking, piracy, or copyright infringements. Tanthawi (2014) suggests a new type of law, more global and borderless, less conventional, whose compliance should be ensured at national, regional and international scales. The objective should be to anticipate, overcome, prevent and eradicate all types of cybercrimes globally. It was also suggested that the enforcement of such new types of cyber laws in the Indonesian context, should focus more on tracking and anticipating the innovative criminal elements used by cyber criminals and also identify the limitations and shortcomings of the regulations. Tanthawi (2014) also suggested to protect victims of cybercrime with high priority. The law enforcement agencies should develop high expertise and make use of high of information technology, data informatics and forensic sciences.

Use of information technology

The use Information technology to prevent cybercrimes should now take steps further than its conventional functions of storage, networking and connecting devices, infrastructure, and processes to create, secure, exchange, or access digital data. The use of information technology has definitely raised the status of cybercrime to a kind of transnational crime, which does not recognize borders and is global in form, content, application and impact. The advancement of Information technology and the availability of innovative methods of hacking and data infringements, has provided Cyber Criminals with such criminal elements that are difficult to track, anticipate and prevent from taking place. Cyber Crime and Information Technology aim to focus on all aspects of cybercrime, internet frauds, identity theft, etc. in order to contribute to better understanding of the

Internet frauds and cybercrime and the use of information systems in storage, protection and sharing of digital information (Fahlevi et al., 2019; Irfan et al., 2018; Lisdiyono & Mulyani, 2021).

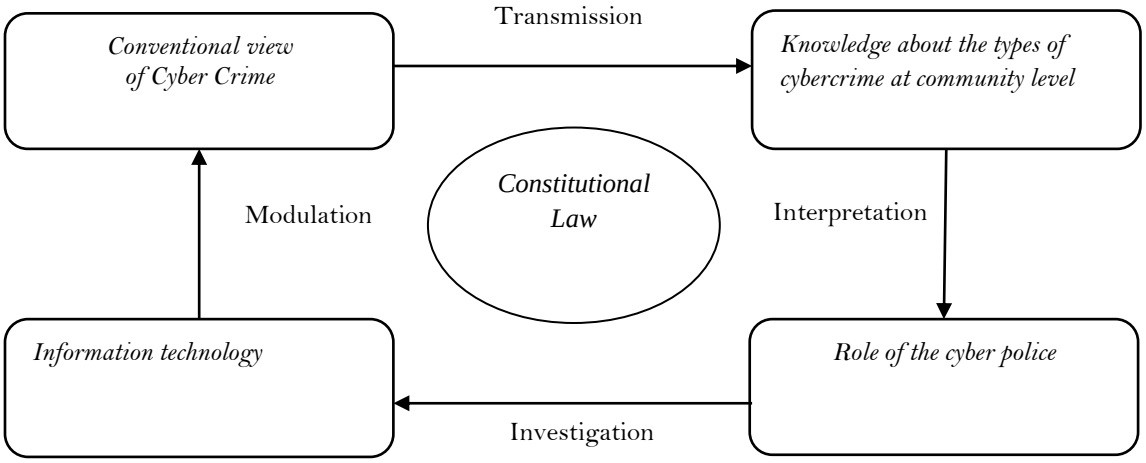
Role of Cyber Police

The Legal, Political, and Security Affairs Ministry in Indonesia promised that cyber police would be fully activated in Indonesia by 2021 (Brewer et al., 2018).) [4] the presence of cyber police is the testimony of the government's initiatives into preventing cybercrimes. Historically, the Indonesia Cyber Police was constituted as a team under Indonesia Criminal Investigation Agency (Bareskrim Polri), also known as Cyber Crime Directorate (Dittipidsiber). Its task was to enforce the law against cybercrimes in Indonesia but not to interfere in the functions of another agency, called Badan Siber dan Sandi Nasional (BSSN), which was primarily responsible to build laws and regulations of cybersecurity.

The cyber police., often termed as National Cyber Security Agency in some countries were exclusively assigned the task to stop *cyber*crimes such as hacking, data manipulation, web phishing, and cyberattacks against digital security system (Fahlevi et al., 2019; Protrka, 2021). In addition, its duty was also to ensure the safety of cyberspace from the spread of hoax, slander, and hate speeches that might disturb the peace of the Indonesian people. People have concerns about the powers and functions of the cyber police. It is often feared that cyber police may be a threat to the freedom of speech as often the cyber police act repressively. This argument was supported by the data released by Statistics Indonesia (Badan Pusat Statistik–BPS), citing that while the Indonesian Democracy Index increased, the level of civil freedom has decreased (CNN Indonesia, 2020). This fear was also found evident in an internal survey conducted by The National Commission on Human Rights (Komnas HAM) involving 1.200 respondents across 34 provinces. The survey found that 36.2% of Indonesian citizens feared to express their opinions freely on online platforms and social media (Republika, 2021).

Theoretical Framework and Research Methodology

The theoretical framework of this study (Figure 1) is based on constructs such as conventional views of cybercrime; knowledge about the types of cybercrime at community level; role of the cyber police and use of information technology for its investigation. The study aimed to highlight how these constructs assist the constitutional law provisions in Indonesia.



The framework clearly presents how the constitutional law supervises the transmission of the conventional view of cybercrimes until it is established in the knowledge at the community level. The Law also helps the community to interpret and assist in the investigation of any problems and inequalities, with the help of cyber police and information technology aids. This is consistent with a view held by Agus and Riskawati (2016), who highlighted how the lack of understanding and knowledge about the types of cybercrime at the community level can cause obstacles in resolving cybercrime and create legal constraints.

The study adopted a qualitative research design, explorative in nature, based on documentation surveys and analysis of legal tools under the Indonesian Law. The data was meticulously collected from various documents related to Cyber criminology and Informational Technology, found in legal case reports and constitutional laws currently in force in Indonesia.

Results

In a survey conducted by the Indonesian Internet Network Organizing Association (CHANIAGO & SAYUTI, 2022), it was found that over 137 million Indonesian people were connected to the internet, a number which was expected to reach 160 million by the year 2020. The reason for this increase in internet users is the ease of access to the internet and computer devices. With such a huge number of internet users, the State Cyber and Code Body (BSSN) designed the Indonesian Security Strategy and circulated to all national security stakeholders. Among these strategies, a few dealt with cyber law and cybercrimes. In compliance with these strategies, the Indonesian Government issued Presidential Regulations Number 53 and 133 of 2017 citing the decisions of the BSSN. These regulations emphasized the need to carry out effective and efficient security measures of the digital data, particularly that was related to economy and national security.

Earlier, in 2005, an initiative was taken to establish Id-SIRTII / CC (Indonesian Security Incident Response Team on the Internet Infrastructure / Coordination Centre) comprising IT practitioners from industry, academia, and government. The primary task of ID-SIRTII / CC was to break the conventional view of the internet security and educate the community about IT Security measures, including how to detect cyber threats. The agency collected log file databases and internet security statistics in Indonesia to give its recommendations. ID-SIRTII has tried to avert the threat of cybercrimes by making a positive use of E-Commerce and establishing cybersecurity systems with the help of e-Commerce business companies (Lukitasari, 2017; Rahmawati, 2017). Besides there are two other investigating agencies that deal with the crimes related to IT and Internet. The first is the Directorate of Special Economic Crimes (DIT TIPPID EKSUS) at the Indonesian National Police Headquarters, which deals with cybercrimes and information and electronic transactions. The second is the Directorate of Criminal Investigation, or the Metro Jaya Regional Police, whose task was to conduct investigations for the crimes related to IT, telecommunications, and electronic transactions. In spite of these agencies and investigating directorates, there is a continuous increase of internet fraud and cybercrimes. Cybercrimes continue to increase and affect the individuals and businesses. Apart from the individuals falling prey to hackers and cyber criminals, the companies are losing their intellectual wealth, resulting in the enormous losses of profits (Jhon, 2018).

Conventionally, like any other country, Indonesia too focused its efforts to prevent cybercrime only on information and electronic related transactions, assuming that it will regulate all cyber related crimes. However, this conventional view increased difficulties and

inequalities and created several complications in the investigation process. Indonesia, which depended strongly on its Law No. 11 of 2008 for all types of Internet and Electronic Transactions, now felt to revoke and amend this law. This Act was amended twice, first, as Government Regulation No. 82 of 2012 concerning the Implementation of Electronic Systems and Transactions; and later amended as Law No. 19 of 2016 Amendment, concerning Electronic Information and Transactions. There were two other additions to the Law, namely Permen Kominfo No. 10 of 2015 and Permen Kominfo No. 7 of 2018 concerning Procedures for Registration of Electronic Systems in the State Administration (Wulandari, 2018). In spite of these laws, enforcement of law against criminals is still very minimal, making cybercrime free in Indonesia. It is high time that the government takes serious initiatives to prevent cybercrimes otherwise it would start making adverse impact on nation's economic health.

In 2014, Indonesia conducted a Convention on Cybercrime in Jakarta which stipulated that each member nations shall take legislative measures to stop cyber- criminal offenses particularly which infringes security measures, which obtains computer data via dishonest intentions or takes illegal access to personal and company data. The convention came out with suggestions like utilizing electromagnetic emissions from a computer system while computer data is illegally stolen. (Putra, 2014; Rondelez, 2018). What Indonesia needs is harmonization of all existing legal provisions, acts and constitutional practices on cybercrimes and apply all these to formulate a harmonized, integrated Criminal Law policies to prevent cybercrimes (Jerome, 2020; Sung, 2018). The role of the cyber police is also significant tin controlling cybercrime cases. It is necessary that the prosecution of cybercrime cases by the police must not be supervised by the legal agencies. Cybercrimes are growing so fast that there cannot be any constitutional remedies always available, creating a challenge to the investigators. The community also lacks a complete knowledge of cybercrimes and therefore allows such crimes to happen due to oversight (Agus & Riskawati, 2016).

Conclusion

This study was based on a few premises that Indonesia holds a conventional view of cybercrime; the community lacks a complete knowledge of cybercrimes; that the cyber police have a lot of limitations and constraints; and information technology is not adequately exploited to investigate cybercrimes. Moreover, in the absence of adequately strong constitutional laws against cybercrimes in Indonesia was further a focus on this study. Using the documentation survey and explorative methodology, this paper studied a few constitutional laws in the Indonesian legal system related to cybercrimes. The results and findings proved the premise that the current Indonesian laws related to prevention of cybercrimes were inadequate, primitive and required advanced technology to predict how cyber criminals execute crimes.

The domain of cyber criminology in Indonesia needs overhauling to prevent cybercrime was realized long back in 2008 when a few laws such as such as Law No. 11 of 2008 was enacted for Internet and Electronic Transactions. This was the beginning to the realization of the need for laws and legislations for the cybercrimes, and it led to several such subsidiary laws in next few years. These acts and legislations are very broad in nature and covered a wide scope of crimes related to consumer protection, data protection, intellectual property, e-commerce, electronic contracts, but less concerning severe types of cybercrimes like cybersquatting (domain name related case). However, in 2017, the Indonesian Government established the National Cyber and Crypto Agency, an agency to control cybercrime and to offer cyber defense to victims against all malware, spams, phishing and hacking threats.

Cybercrime is a great threat to the world economy causing a loss of $ 1.5 Trillion each year. The digital business in Indonesia is also under a great threat by cyber criminals and the lack of a robust legislations further aggravates the issue. It is strongly recommended that the Indonesian government should give serious attention to these issues and enact or amend regulations as needed or create institutions that could support in the implementation of these legislations. Cybercrime is like any other transnational crime and hence it is required to harmonize efforts to curb this menace at international levels. Regional groups for cooperation may be formed with the most affected countries as members in all regions of the world (Bande, 2018).

References

Agus, A. A., & Riskawati, R. (2016). Penanganan Kasus Cyber Crime Di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar). *SUPREMASI: Jurnal Pemikiran, Penelitian Ilmu-ilmu Sosial, Hukum dan Pengajarannya, 11*(1). https://doi.org/10.26858/supremasi.v11i1.3023

Arifah, D. A. (2011). Kasus cybercrime di indonesia. *jurnal Bisnis dan Ekonomi*, *18*(2), 185 – 195. https://unisbank.ac.id/ojs/index.php/fe3/article/download/2099/767

Bande, L. (2018). Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities. *International Journal of Cyber Criminology, 12*(1), 9-26. https://doi.org/10.5281/zenodo.1467632

Brewer, R., Cale, J., Goldsmith, A., & Holt, T. (2018). Young people, the internet, and emerging pathways into criminality: A study of Australian adolescents. *International Journal of Cyber Criminology, 12*(1), 115-132. http://dx.doi.org/10.5281/zenodo.1467853

CHANIAGO, H., & SAYUTI, A. M. (2022). The Impact of Social Media Use on Student Entrepreneurship Intention and Implementation: Evidence from Indonesia. *The Journal of Asian Finance, Economics and Business, 9*(2), 371-382. https://doi.org/10.13106/jafeb.2022.vol9.no2.0371

CNN Indonesia. (2020). Kebebasan Sipil Turun, Indeks Demokrasi Indonesia Naik. https://www.cnnindonesia.com/nasional/20200803160536-32-531684/kebebasan-sipil-turun-indeks-demokrasi-indonesia-naik

Daryono, D., & Sugiantoro, B. (2017). Pengembangan Framework Pelaporan Cyber Crime. *JISKA (Jurnal Informatika Sunan Kalijaga), 1*(3), 133-147. https://doi.org/10.14421/jiska.2017.13-05

Dmello, J. R., & Bichler, G. (2020). Assessing the Impact of Civil Gang Injunctions on the Use of Online Media by Criminal Street Gangs. *International Journal of Cyber Criminology, 14*(1), 44-62. http://dx.doi.org/10.5281/zenodo.3739876

Fahlevi, M., Saparudin, M., Maemunah, S., Irma, D., & Ekhsan, M. (2019). Cybercrime Business Digital in Indonesia. *E3S Web of Conferences. 125* (pp. 21001). EDP Sciences. https://doi.org/10.1051/e3sconf/201912521001

Hegazy, S. M. A. (2021). Terminating The Public Employee's Service Due to Lack of Health Fitness and Proven Drugs Abuse or Addiction in The Light of The Criminal and Civil Service Laws in Egypt and Saudi Arabia. *International Journal of Criminal Justice Sciences, 16*(2), 49-68. http://dx.doi.org/10.5281/zenodo.4756491

Irfan, M., Ramdhani, M., Darmalaksana, W., Wahana, A., & Utomo, R. (2018). Analyzes of cybercrime expansion in Indonesia and preventive actions. *IOP Conference Series: Materials Science and Engineering. 434*(1) (pp. 012257). IOP Publishing. https://doi.org/10.1088/1757-899X/434/1/012257

Ismail, D. E. (2009). Cyber Crime di Indonesia. *Jurnal Inovasi, 6*(03), 242-247. https://ejurnal.ung.ac.id/index.php/JIN/article/view/815

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International journal of cyber criminology, 1*(1), 1-6. http://cybercrimejournal.sascv.org/editorial.htm

Jerome, B. (2020). Criminal Investigation and Criminal Intelligence: Example of Adaptation in the Prevention and Repression of Cybercrime. *Risks, 8*(3), 99. https://doi.org/10.3390/risks8030099

Jhon, R. M. (2018). Existence of Criminal Law on Dealing Cyber Crime in Indonesia. *IJCLS (Indonesian Journal of Criminal Law Studies), 3*(1), 25-34. https://doi.org/10.15294/ijcls.v3i1.16945

Juditha, C. (2016). Communication Patterns in Cybercrime (Love Scams Case). *Jurnal Penelitian Dan Pengembangan Komunikasi Dan Informatika, 6*(2). https://jurnal.kominfo.go.id/index.php/jppki/article/view/592

Ketaren, E. (2016). Cybercrime, Cyber Space, dan Cyber Law. *Jurnal Times, 5*(2), 35-42. https://ejournal.stmik-time.ac.id/index.php/jurnalTIMES/article/view/556

Lisdiyono, E., & Mulyani, S. (2021). Implications of Legal Positivism on Cybercrime Law Enforcement in Indonesia in the Case of the Hacking of the Mojokerto City Government Website. *International Journal of Criminology and Sociology, 10*, 891-896. https://doi.org/10.6000/1929-4409.2021.10.105

Loader, B. D., & Thomas, D. (2013). *Cybercrime: Security and surveillance in the information age*. Routledge. https://dl.acm.org/doi/abs/10.5555/555946

Lukitasari, D. (2017). Problems of Creation Crime Through the Use of Democratic Database Systems in E-ID. *IJCLS (Indonesian Journal of Criminal Law Studies), 2*(2), 102-110. https://doi.org/10.15294/ijcls.v2i2.12316

Nasrollahzadeh, S., & Koramaz, T. K. (2020). Residential satisfaction and mobility in Göktürk peripheral neighbourhood. *socialspacejournal.eu, 20*(2), 51-84. http://socialspacejournal.eu/Social%20Space%20Journal%2022020(20).pdf#page=51

Protrka, N. (2021). Cybercrime. In *Modern Police Leadership* (pp. 143-155). Springer. https://doi.org/10.1007/978-3-030-63930-3_13

Putra, A. K. (2014). Harmonisasi Konvensi Cyber Crime dalam Hukum Nasional. *Jurnal Ilmu Hukum Jambi, 5*(2), 43297. https://www.neliti.com/publications/43297/harmonisasi-konvensi-cyber-crime-dalam-hukum-nasional

Rahmawati, I. (2017). the Analysis Ofcyber Crime Threat Risk Management To Increase Cyber Defense. *Jurnal Pertahanan & Bela Negara, 7*(2), 37-52. : https://www.researchgate.net/publication/330665151

Republika. (2021). Survei Komnas HAM Ungkap Ketakutan Warga Kritik Pemerintah. https://republika.co.id/berita/qmcp8j409/survei-komnas-ham-ungkap-ketakutan-warga-kritik-pemerintah

Rondelez, R. (2018). Governing cyber security through networks: an analysis of cyber security coordination in Belgium. *International Journal of Cyber Criminology, 12*(1), 300-315. http://dx.doi.org/10.5281/zenodo.1467929

Sari, P. B., Rossanty, Y., & Nasution, M. D. T. P. (2018). CYBERCRIME CASE ON SOCIAL MEDIA IN INDONESIA. *International Journal of Civil Engineering and Technology, 9*(7), 783–788. http://www.iaeme.com/ijciet/issues.asp?JType=IJCIET&VType=9&IType=7

Sung, Y.-H. (2018). Book review of cyber bullying approaches, consequences and interventions. *International Journal of Cyber Criminology*, *12*(1), 353-361. 10.5281/zenodo.1467944

Tanthawi, D. (2014). PERLINDUNGAN KORBAN TINDAK PIDANA CYBER CRIME DALAM SISTEM HUKUM PIDANA INDONESIA. *Jurnal Ilmu Hukum*, *2*(1). http://www.e-repository.unsyiah.ac.id/MIH/article/view/4574

Tianotak, N. (2011). Urgensi cyberlaw di indonesia dalam rangka penangan cybercrime disektor perbanka. https://fhukum.unpatti.ac.id/download/jurnal-paper/sasi/JURNAL%20SASI%20VOL.17%20NO.4%20OKTOBER-DESEMBER%202011/3

Wulandari, D. (2018). EX ANTE REVIEW dalam Mewujudkan Konstitusionalitas Peraturan Perundang-Undangan di Indonesia. *Indonesian State Law Review (ISLRev)*, *1*(1), 37-52. https://doi.org/10.15294/islrev.v1i1.26938

Yar, M. (2005). Computer hacking: Just another case of juvenile delinquency? *The Howard Journal of Criminal Justice*, *44*(4), 387-399. https://doi.org/10.1111/j.1468-2311.2005.00383.x

Yasutomi, A. (2020). When Soldiers Speak Out against Their Own Military : A Study of Non-Academic Books Published by Retired Japanese Officers. *Res Militaris*, *10*(1), 1-21. https://resmilitaris.net/index.php/2020/01/01/id1031546/