Harmonization of Cyber Crime laws with the Constitutional Law in Indonesia

M. Erham Amin[1]
Universitas Lambung Mangkurat, Banjarmasin, Indonesia

Mokhamad Khoirul Huda[2]
Universitas Hang Tuah, Surabaya, Indonesia

Abstract

The current study aimed to examine the harmonization of cybercrime in the Indonesian constitutional law by reviewing its status. The focus of this study was on different aspects of cybercrime in the constitutional law and to find out the extent to which harmonization of cybercrime has taken place. The study adopted sociological research approach along with the application of the theory of law enforcement. The legal aspects of law enforcement policies for cyber security and proving cybercrime were used to conduct the review and analysis. These legal aspects are firmly documented in various Indonesian regulations and laws, such as Indonesian Criminal Code, Act 11 of 2008, Act 19 of 2016, and the Constitutional Law code number 20/PUU-XIV/2016. The 2001 Convention on the cybercrime proposed by European Union had emphasized the harmonization of Indonesian cybercrime regulations with the international regulations and constitutional law. The policies of law enforcement that were to be harmonized and applied for cybercrime minimization involved both penal and non-penal approaches. Some of the policies were strictly specific to the public sector, or the private sector or the military so there is yet a significant requirement of further harmonization of the cybercrime, in the constitutional law while focusing on all of the sectors and bodies equally.

Keywords: Harmonization, Cyber Crime, Constitutional Law, Indonesia

Introduction

Scholars have elaborated that the world has seen a rapid transformation with respect to technological advances around the globe (Jang, 2013). The recent decade is full of technological changes which have affected the whole of humanity living on earth. Broadhurst and Chang (2013)has revealed the fact that the universal life of the whole society

[1] Department of Law, Universitas Lambung Manggkurat, Banjarmasin, Indonesia.
E-mail: muhammad.erham@ulm.ac.id
[2] Faculty of Law, Universitas Hang Tuah, Surabaya, Indonesia.
E-mail: emka.huda@hangtuah.ac.id

is impacted by the advances made by different stakeholders through technology. Technological advancement although has changed the lives of people but it has also some precious consequences which may prove much more harmful (Aditya & Al-Fatih, 2021; Altayar, 2017). The continuous changes in society are being done through the acceleration of information technology and the interactions of society while technology expanded greatly. Furthermore, many studies have separately emphasized that the use of technology is indispensable in everyone's life as without this no person can survive (Maskun et al., 2021). Even to participate in social events effectively, people need to respond to technology rapidly.

In the world of the internet where every individual is carrying the latest gadgets and technological means, communication has become easier than ever (Rahmawati, 2017). In addition to this, internet has changed the whole world and brought the globe at one click and every movement of the people may be tracked through technology usage. The internet and technological advances have removed the limits that existed before (Arief, 2006; Azmi, 2020). Rapid business growth and information transfer has become possible through the network during the current decade. The growing usage of technology and related equipment has caused much growth of the economic contribution by the firms and individuals dealing in business. With the help of telecommunication technologies in different parts of Asia, the world has seen the rapid growth of businesses in such countries (Schjolberg, 2008). All territories or boundaries of almost every country have been removed with the implementation of the means of information technology. The rapid transformation of information from one end to another has been possible by the use of technological means of communication, which has made business operations smooth (Broadhurst & Chang, 2013; Bunga, 2019).

Several studies have argued the sensitive issue of cybercrime, which has grown multi-dimensionally with the latest adoption of technology. Concerns have been generated by various individuals and firms over the issue of cybercrime at different levels. This has given the rise to the need to introduce cyber laws to counter cybercrimes around the world (Chawki et al., 2015; Choirunnisa, 2021). Cyber laws have gained international importance and value as these laws were first enforced in European countries with most supporters. Cyber laws are basically designed to counter cybercrimes and present such regulations and rules that may offer some relief to the people from such crimes (Christianto, 2020; Djanggih, 2018b).

Due to increased number of complaints in Indonesia, the cybercrime wing introduced the telematics law which aimed to control situations of mishaps over telecommunications in the country (Zulfikar et al., 2020). This law is also of international importance as various cyber laws, media laws, and information technology laws are part of this law, and it has also been recognized across the world. In the year 2019, the Indonesian national cyber and crypto agency presented a report presenting the figure of 290 million cases related to cyberattacks in the country (Djanggih, 2018a; Djanggih et al., 2018). This represented 25% enhancement in cyberattacks in comparison with the attacks of previous years. The losses due to cybercrimes also crossed 34.2 billion U.S. dollars for Indonesia (Djanggih, 2018a; Djanggih et al., 2018).

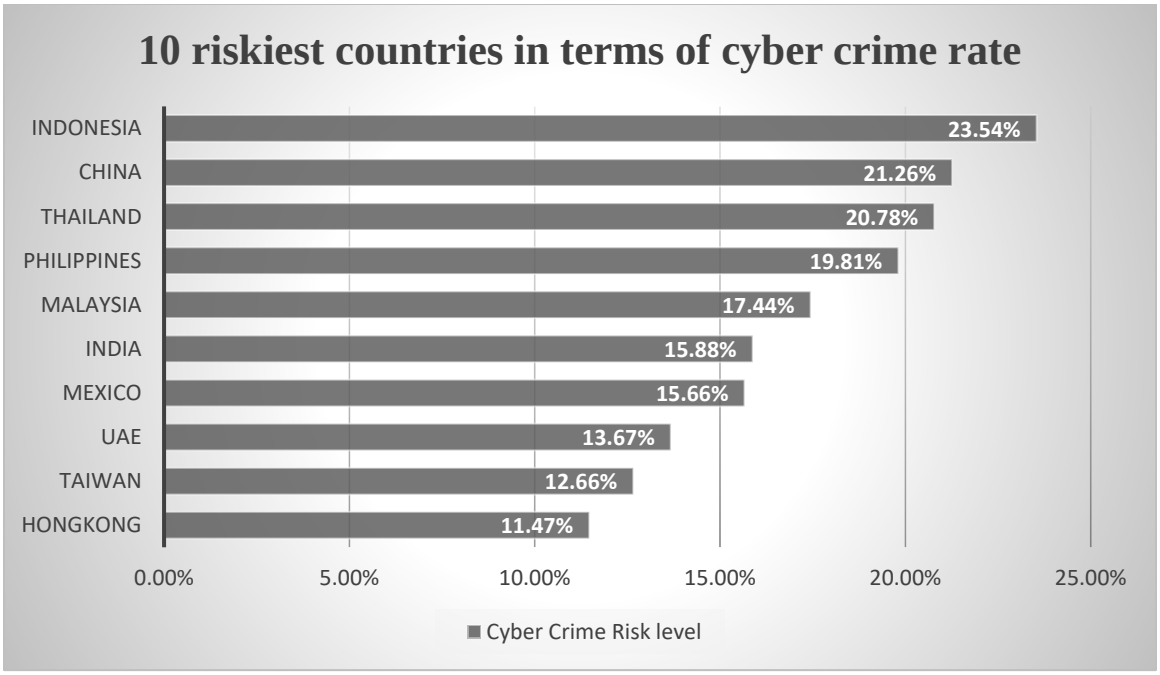

Figure 1: 10 riskiest countries in terms of cybercrime rate
Source: (Aditya & Al-Fatih, 2021)

Figure 1 presents the data of 10 riskiest countries in terms of enhancing cybercrime rates, in which the highest rate is for Indonesia. This means that cybercrime rates in our country are of great concern. In such a state, the harmonization of cybercrime with the constitutional law is therefore significantly required in order to significantly decrease cybercrime rate in the country (Djanggih et al., 2018; Dwipayana et al., 2020).

As a result of the pandemic of COVID-19, significant enhancement in the phishing cyber-attacks has been observed. In addition, there are also ransomware attacks, mal-spams and various cyber-attacks that have created an urgency to establish a well-functioning infrastructure that can tackle cybercrimes and the issues of cyber security in the country (Ersya, 2017; Fahlevi et al., 2019). Before the usage of the internet, activities were national but with the usage of internet and information technology, the national activities have now changed into international. Precautionary measures are therefore needed to counter the upcoming challenges.

The hackers or cyber-criminals who misused the technological advancements and harassed the victims belonged to various countries, which posed bigger challenges to law enforcement agencies. All the transactions were carried out from computers through the internet access. All such crimes need the involvement of law agencies of more than one country (Jaelani & Luthviati, 2021). There are two parties involved in a cybercrime, the hacker committing the crime and the victim. Cybercrime is different from each perspective. Even the crime scene is different than the normal and regular crime. Hence, laws must also be different to tackle situations of cybercrimes (Karo & Sebastian, 2019). Besides, cybercrimes need serious handling and professional teams to carry out the whole investigations, who may face great challenges in the field. In order to have deep insight into such sensitive topics, people need to do deep insight research to know the clear situation (Kshetri, 2013). This means that there is a need to have a clear picture of the Indonesian criminal procedure and verify whether cyber threats are genuine or not.

Various efforts have been made through different channels in the country to control and check cybercrimes. However, law enforcement agencies consider the enactment and implementation of cybercrime laws as the only solution. A few excerpts of cyber-crime laws were presented by the UN in 2000, but they were of no match with the provisions of the Indonesian criminal law system and therefore no harmonization could take place (Faiz, 2016; Hakim et al., 2018). This topic has also been discussed in the Indonesian Parliament and all stakeholders have been talked and discussed the pros and cons of the cybercrime law (Hatta, 2020; Hermawan, 2015).

Various practitioners and experts have proposed a dire requirement of cyber security bill that should clearly delineate and defines the responsibilities, roles and authorities of various institutions and fully addresses the threats and problems related to cyber security (Nurahman, 2020; Prahassacitta, 2016). Keeping in mind the importance of cyber security and significantly observing the cyber threats in Indonesia, various studies have proposed that the Indonesian national cyber and crypto agency and the Indonesian parliament must engage in a public-private dialogue to deliberate a cyber-security bill. Such a public private dialogue can result in sharing of relevant knowledge, information and experiences of various people for producing workable and sensible policies, and would later be supported by stakeholders as well (Prayudi et al., 2015; Saputra, 2016).

In 2019, one of the initiatives included the revision of the Electronic Transaction Law, 2008, attempting to govern the electronic informational technology transactions. In the criminal justice process, the late provisions of a law are very accommodating (Hatta, 2020; Hermawan, 2015). Chang (2020) disclosed that this law proved useful as many threats were removed by the law enforcement agencies and the criminal agencies' processes were clear to the public as well. The latest provisions and regulations of this law were based on correct evidentiary system and legal principles (Indrajit, 2016).

Till date no research study has significantly focused on the current situation of cyber security and cybercrime in Indonesia. As a result, the government has not yet come out with any practical implications or policies for the eradication of cybercrime (Setiadi et al., 2012). Moreover, authors and experts have not significantly focused on finding the reasons for the increase in cybercrime rates in Indonesia, and why cyber security is vanishing away slowly (Setiadi et al., 2012). There is also a significant need to analyze cyber security regulations and laws present in Indonesia currently. It is important to study and analyze the feasibility of harmonization between cyber security regulations and the constitutional laws of Indonesia. It is also required to study the possibility of alignment between the public and private sectors, for the implication of cyber security laws and regulations (Smith & Perry, 2021; Suhariyanto, 2014).

This research study aimed to fill all these research gaps and focused on different aspects of cybercrime in the Indonesian constitutional law and to find out the extent to which harmonization of cybercrime can take place. The study premised that law enforcement policies if harmonized with cybercrime procedures should involve both penal and non-penal approaches, equally applicable to public and private sectors. The next section presents the review of literature, followed by the section on research methodology. The results, discussion and analysis are presented in the next section. The final section contains a conclusion and recommendations.

Literature review and theoretical base

Definition of cyber crime

Generally, the term cybercrime or computer cybercrime is referred to as efforts done by an individual for entering and using computer networks and the computer facilities without any kind of permission, against the law, and with the purpose of making or not making any kind of damage or changes to the computer. Cybercrimes are any actions or any words through any party that can threaten the national security, territorial integrity and national sovereignty (Abdul Wahid & M Labib, 2005; A Wahid & M Labib, 2005; Wild et al., 2011; Yusa, 2017). Kshetri (2013) defined cybercrime as a crime which involves utilization of computer as a major instrument for furthering of illegal ends, involving commitment of fraud, stealing of intellectual property, trafficking in the case of child pornography, stealing of important information, identities, and the violation of privacy of an individual or organization. In another study, cybercrime is described as involving criminal activities that are committed and carried out with the help of the Internet or the computers, which result in various kinds of crimes such as cyber extortion, identity theft, data breach and harassment of the individual being exploited (Kshetri, 2013; Lagazio et al., 2014).

Cybercrime in Indonesia and need for regulations

In the recent years, the significant development in information and communication technologies (ICTs) has resulted in positive and significant global economic growth and development. Due to competitiveness, productivity and significant engagement of people and systems, businesses and agencies are more connected than ever in the cyberspace. This poses new challenges in the forms of cyber threats, with increasing numbers of cyber criminals (Dhanapal et al., 2020; Muthia & Arifin, 2019; Naro et al., 2020). As stated earlier, in the year 2019, the Indonesian national cyber and crypto agency had identified 290 million cases related to cyber-attacks in the country (Djanggih, 2018a; Djanggih et al., 2018),which was 25% increase in comparison with the previous year, amounting to losses worth 34.2 billion U.S. dollars for Indonesia.

The situation grew worse as a result of the pandemic, as significant increase in phishing cyber-attacks, ransomware attacks, mal-spams and various cyber-attacks were observed. This necessitated the establishment of a well-functioning infrastructure that could try to curb the cybercrimes and resolve the issues of cyber security in the country (Djanggih, 2018a; Djanggih et al., 2018; Salavrakos, 2020). The Indonesian cyber security regulations, rules and laws focus only on the fragmented responsibilities related to various ministries. However, these are remaining ineffective up till now for preventing the cybercrime in the country and the continuous cyber threats being received by the governments and corporations as well (Bryan, 2020; Muthia & Arifin, 2019; Naro et al., 2020).

There is also a significant requirement of comprehensive regulations for the minimization of cybercrimes and enhancement of cyber security (Naro et al., 2020). The Indonesian parliament worked on overarching cybersecurity bill however, the procedure did not involve significant covering of the cybercrimes presently prevailing in the private sector (Nurahman, 2020). As a result of this, the bill contained provisions that were significantly costly for most of the businesses and cumbersome. It also required various accreditations, certifications and approvals from the BSSN for the development of products and services of cyber security (Prahassacitta, 2016; Prayudi et al., 2015). The bill had also ignored the local content requirements which had greatly enhanced the level of risk to cyber security in Indonesia. For this reason, the bill was significantly criticized at various levels. Consequently, it was withdrawn from the agenda of the parliament for both the years 2020 and 2021 (Krysiński & Szczepański, 2020; Naro et al., 2020).

Indonesia's Cybersecurity regulations

The workability and practicality of cyber security regulations and laws are very important for practitioners, as a result of which, deliberating a bill would result in workable and sensible laws and regulations for cyber security for both the public and private sector in Indonesia (Smith & Perry, 2021; Suhariyanto, 2014). To grant it a legal basis, and to initiate the cyber security regulations in Indonesia, the Electronic Information and Transaction (EIT) Law No. 11/2008, was revised as Law No. 19/2016, though the experiment failed soon (Sunkpho et al., 2018; Tapsell, 2019). The revised law was applicable only on various kinds of offences in Indonesia which were otherwise prohibited such as breach of data protection, distribution of illegal content, unauthorized access to personal information of individual, or stealing the corporate content (Sunkpho et al., 2018; Tapsell, 2019). It also covered unauthorized and illegal wiretapping and interception of computer and electronic systems, involving various breaches related to the computer and information systems (Tosoni, 2018; Ulima, 2018).

Although the EIT law provided significant legal protection related to electronic transactions and electronic systems, but it did not cover significantly the urgent and significant aspects related to cyber security, such as building a safe and protected network, creating information infrastructure and recruit skilled cybersecurity experts to fight with the cybercrimes. Moreover, the EIT Law approved in 2016 soon became redundant since all its technical regulations related to the implementation of electronic transactions and systems were included in government regulations known as the GR 71/2019 (Tapsell, 2019; Ulima, 2018). The GR 71/2019 also contained r the electronic transactions and systems.

Apart from various articles related to offences which were already regulated by the EIT Law of 2016, the updated Law GR 71/2019 contained significant provisions related with the protection of personal information and data. It also mandated website authentication for avoiding any kind of scam, fraudulent or fake activities related to the websites (Tapsell, 2019). Besides, the GR 71/2019 also stressed upon the need for the government to preventing any such situation that can harm public interests due to the misuse of electronic transactions and electronic information. The Law also emphasized upon the requirement of a separate national cybersecurity strategy in Indonesia (Tapsell, 2019).

The GR 71/2019 covered cybercrimes in a very limited manner. Since the emphasis in the Law was on regulations related to electronic transactions, the Law was strict on the misuse of data and information, or the spread of malicious codes and electronic content under unauthorized electronic signatures (Tapsell, 2019). The Law did not directly talk about implementation of cyber security related regulations. This limited coverage of the cybersecurity related regulations was a significant drawback of the Indonesian government to tackle the cyber security related problems. For this reason, till date the cyber security related laws and regulations could not be significantly harmonized nor adequate attention has been given to all kinds of cybercrimes and the problems related with cyber security.

The coverage of the GR 71/2019 was also inadequate in comparison with the response of other countries to check cyber threats, specifically the threats that are faced by large corporations and by the critical infrastructure of the government of Indonesia (Ulima, 2018; Abdul Wahid & M Labib, 2005; A Wahid & M Labib, 2005). However, in order to deal with the cyber threats received by national security, there was also Ministry of Defense Regulation No. 82/2014 which provided various cyber defense guidelines. This was the

most prominent regulation that significantly defined cyber security in Indonesia but being developed and implemented by the Ministry of Defense, these guidelines and regulations were only focused on national armed forces (Tosoni, 2018; Ulima, 2018). However, unlike the EIT law, this set of guidelines was significantly covering the critical infrastructure of the corporations and governments, like covering the financial and transportation systems, by considering then the objects related to cyber security (Tosoni, 2018; Ulima, 2018). Moreover, these regulations only served the military and were focused on the development of military cyber defense. What Indonesia requires is a system that could secure all the information and data and then support the infrastructure from cyber-attacks in Indonesia at national level.

It seems that both laws were directed at the private sector or largely covered the defense and military matters, except a few regulations that mentioned public corporations (Tapsell, 2019). In all these cases, there was a lack of harmonization with the laws related to cybercrime and cyber security. It is therefore a need to focus on the development of cyber security and cybercrime related laws and regulations which are directly related with the constitutional law and are harmonized over every sector, corporation and body present in Indonesia (Aditya & Al-Fatih, 2021).

Theory of law enforcement

Various new kinds of crimes, which are of transnational nature, have resulted from the use of the Internet and computers. With the increase in the number of these crimes, the Indonesian government requires a novel international legal instrument that can be utilized and applied for the dealing of cybercrime cases and establish a cyber-security system with international legal norms (Aditya & Al-Fatih, 2021; Altayar, 2017). Due to the advancement of the Information Technology sector, it is much easier for cyber-criminals to violate the law. With the usage of the Internet network, cybercrime can be directly expanded to an international level. There are two different categories of cybercrimes: one which is committed in a broad sense; second, which is committed against already existing systems (Bunga, 2019). The broad sense of cybercrimes includes crimes against all the global network systems and individuals that are using computer software media at any point of time.

Considering the review of literature and the context of the problem under study, the theory of law enforcement can be applied. This theory focuses on the harmonization of cybercrime related laws and regulations with the constitutional law, when there is a need for the enforcement of law. In other words, it recognizes that when required the harmonization of laws should be executed on every individual, sector and corporation in Indonesia (Azmi, 2020). The hypothesis proposed in this regard involves scientific writing, which proposes that, "The legal aspects of cybercrime have been firmly regulated in several laws and regulations in positive law in Indonesia." Hence, with the application of the law enforcement theory, it would be easier to harmonize these laws. The harmonization of this type with the application of law enforcement theory to resolve cybercrime problem in Indonesia can be carried out with both non-penal and penal approaches (Djanggih, 2018b). For instance, there is a reference to law enforcement in Indonesian Criminal Procedure Code, Act No 19 of 2016 (Azmi, 2020). A few of its provisions are related with cybercrime and are harmonized in the international regulations, during the 2001 Conventions on the Cybercrime, proposed by the European Union.

Methodology

This study utilizes the sociological law research method, which is a type of research that significantly focuses on norms and laws, also sometimes called positive legal research. In this type of research, the researcher describes reality in accordance with the data from natural settings, and legal facts that can be observed thoroughly and in detail, as the problem is peeled out in depth to be studied (Djanggih, 2018b). This study also focuses on the current efforts in Indonesia that are being made in order to harmonize the rules and regulations related with cybercrime with the constitutional law. Based on the literature review and observation, this study intended to propose some recommendations regarding harmonization of cybercrime laws with the constitutional law of Indonesia (Aditya & Al-Fatih, 2021).

As a first step of this methodology, this study reviewed the current status of cybercrime laws and regulations in Indonesia. This step revealed the problems and limitations that existed in the Indonesian legal system. As the second step, the study reviewed the international norms as specified in various international conventions related to cybercrime. The third step was to analyze the harmonization process of the current cybercrime laws and regulations with the constitutional law of Indonesia. The final step of this research methodology was to adopt a penal and non-penal approach to identify how to tackle with cybercrimes and to understand the extent to which cybercrimes can be harmonized with the constitutional law in Indonesia.

These steps led to a few recommendations (Choirunnisa, 2021; Christianto, 2020) which were the result of the review and analysis of various legal aspects of proving cybercrime as eligible for law enforcement and harmonization with the constitutional law in Indonesia.

Discussion

Cybercrime proving legal aspects

An important clause in the Act 19 of 2016 Law was related to the regulation of electronic transactions that concerned cybercrime and cyber security. This regulation can be observed to be an implementation of various principles related with international provisions. The Act 19 proposed in 2016 also contained all the prohibited acts mentioned in Article 27 to Article 36 (Aditya & Al-Fatih, 2021; Altayar, 2017; Arief, 2006). The provisions presented in Article 42 also significantly regulated the provisions related with the investigation, which stated, "The investigation referred to in this law is conducted based on the provisions in the Criminal Procedure Code and the provisions in this law" (Azmi, 2020). As a result, the system of evidence that is adopted is referred to as theory of evidence that is based upon the law in negative manner. This phenomenon also involves a system based provision as mentioned in the Article 183 of the criminal procedure code stating that, "A judge must not impose a crime on someone unless with at least two legal pieces of evidence he had gained the conviction that a crime had actually taken place and that the defendant was guilty of it". This means that evidence is supposed to be based on different provisions under the law and should be recorded as a legal evidence in accordance with the article 184 related to the criminal procedure code (Azmi, 2020). The following would be the requirements of producing such evidences in the court of law.

i. Testimony of witnesses

It involves formal requirements related with witness statements as recommended by the criminal procedure court. This is executed through oath appointment. The requirements for such a testimony include (Bunga, 2019):

- No inventions, opinions and expert statements;
- Information must be regarding the event that was heard, experienced or seen by the witness along with the statement of the reason behind the knowledge of the event;
- There must be more than one witness under the application of the principle of *unus testis nullus testis;*
- Information must not be obtained from other people by the witness, applying the principle of *testimonium de auditu;*
- There must be a match between the testimony of two or more witnesses' in terms of information and evidence.

Due to the nature of cybercrimes, which are mostly virtual, the evidence with the help of witness statements is not possible to be obtained directly. Such witness statements can be presented in the form of hearing of other people and conversations (Choirunnisa, 2021). This is presented as the testimony, called as *testimonium de auditum*, or the evidence of hearsay. This type of testimony is not directly used as evidence, in practicality, however, it is considered for presenting to the judge for strengthening the conviction of the judge before decision making (Choirunnisa, 2021).

ii.Statements of experts

This involves an expert who is expert in the field of legal matters and his competence is considered significant. He must also be well-versed with regulations and his statement must be fully supported by formal regulations as evidence. If asked to attend the trial, he must give a statement which is truly elaborate with explanations. He must testify that the electronic data or the documents submitted are completely legal and can be accounted for as evidence in the court of law (Christianto, 2020; Djanggih, 2018b).

iii.Letter of evidence

Various kinds of letters are recognized by a court as evidence, on the basis of which verdicts may be announced. These letters need to be authenticated by officials. The rules regarding such letters of evidence are provided in the Article 184, Letter C and the Article 187, of the Criminal Procedure Code (Dwipayana et al., 2020). These letters are authentic letters that might provide a number of evidences such as proof of payment, names and addresses of agencies that have issued these letters, or the letters of agreement that can be attached for the purpose of legal relationships. All these letters of evidence can be submitted in the court in accordance with the Article 187 of the Criminal Procedure Code (Hatta, 2020).

iv.Defendant's statement

In accordance with Article 184 and Article 189 of the Criminal Procedure Code, the defendant's statements are narrations of actions done by the defendant, known by the defendant or experienced by the defendant (Hatta, 2020). The provision presented in Article 44 states that the defender's statements are "evidence for investigation, prosecution and examination in court according to the provisions of this law are as follows: involving all objects of evidence present in the law; each form of evidence should be in accordance with Article 1, No. 1, 4 and 5 and Paragraph 1, 2 and 3 respectively".

Law enforcement policies for cybercrime

i.The penal approach

According to any criminal policy, a criminal law is not a primary or major policy tool; it is the part of a strategic or any other major policy which aims at preventing or eliminating conditions that cause a crime. In accordance with this perspective, a criminal law cannot

help in tackling cybercrimes, however, a systematic approach may be taken to resolve it (Manihuruk & Tarina, 2020). A workshop was conducted on the computer related crimes by the United Nations Congress to explore the possibility of making use of policies and efforts for tackling the cybercrime, and with the help of a country's criminal law. The major focus of this workshop was to harmonize the provisions related with cybercrime with criminalization, verification and procedures of the constitutional law (Naro et al., 2020). The major problem observed was not only related to making and developing criminal law policies, the problem was also related with the harmonization of the criminal policies all over Indonesia in order to deal with cybercrime. The conduct of this workshop hints at the international acceptance of the need to harmonize the cyber-laws with the constitutional laws.

ii. The non-penal approach

The non-penal approach adopted against cybercrime in Indonesia is related with the concept of Hoe Angels, which involves the prevention of cybercrime without the utilization of punishment, but with other measures such as prevention, community mental health planning, national mental health plans, child welfare plans and social work planning, and if any legal provision needed, utilization and application of administrative and civil law (Nurahman, 2020). The non-penal approach for the prevention of cybercrime according to the constitutional law involves more precautionary measures. The major objective of non-penal approach was to overcome various factors that were conducive to the occurrence or the happening of cybercrimes. It also focused on various social and legal phenomenon that can cause increase in the cybercrime (Tapsell, 2019; Tosoni, 2018).

The non-penal approach also significantly focused on all of the factors and characteristics that must be implemented in order to harmonize cybercrime related laws with the constitutional law, and to minimize this crime by identifying the factors that enhance this crime (Aditya & Al-Fatih, 2021). It is not certain whether the non-penal approach would be effective, but it is sure that cybercrimes require vigilant response and global action, as these crimes are not bound by any borders and can become transnational at any point in the time (Azmi, 2020).

This discussion reveals that both penal and non-penal approaches are significantly contributing towards the harmonization and minimization of cybercrime with the constitutional law and enhancement of cyber security in Indonesia (Christianto, 2020).

iii. The harmonization efforts

Various policies, laws and regulations were forwarded as a result of penal and non-penal approaches to explore the harmonization of cybercrimes with the constitutional law of Indonesia. These efforts and approaches include the following (Choirunnisa, 2021):

- Modernization of formal criminal law and material criminal law to facilitate the harmonization of cybercrime with constitutional law and align the laws with international regulations relevant to crimes specific to the telecommunication sector.
- The national satellite security protection work for the harmonization of cybercrime with the constitutional law by referring to the provisions that are applicable with the international standards.
- Taking the benefit of the expertise of law enforcement officers, regarding the procedure involved in handling of cases including cybercrime and those relevant to the Internet sector.
- Increasing public legal awareness about cybercrime related security and laws.
- Enhancement of the cooperation between all sectors in Indonesia along with

international cooperation, involving bilateral, multilateral and regional cooperation for fighting with the cybercrime.

- Exploring the possibility of interpreting cyber security and cybercrime in accordance with the constitutional law aiming at harmonization and understanding issues of jurisdiction for upholding the state sovereignty.

iv.Electronic Information Laws and harmonization

In Indonesia, the electronic information laws are regulated under the Government Regulation 82, which is related to the implementation of electronic transactions and systems, informatics and communication regulations, and protection of the personal data in electronic systems (Mulyadi, 2008). There are also specific standards related to the violations of cyber security laws and data protection and privacy laws. Regulators are bound by these standards as they are required to present with minimum two pieces of evidence for the purpose of establishing allegation of any kind of criminal violation (Laurensius et al., 2018; Lim, 2013). The current electronic information law aims at the protection of users; hence, it is natural that this law too would favor harmonization of cybercrime and obtain various administrative sanctions needed for such harmonization. These laws can also abrogate any kind of criminal and civil liability related to cybercrime (Lin & Nomikos, 2018; Lintang et al., 2020). The government right now is dealing with these offences with the help of written warnings, temporary dismissals and administrative fines however, the cybercrimes need to be addressed with a much powerful agenda and opposing laws and regulations (Mansur & Gultom, 2005).

In order to harmonize the cybercrimes and cyber security as well with the constitutional law, the cybercrime unit of the Indonesian police is working vigilantly as well, focusing on preventing crimes such as defamation of character, hoaxes, malicious comments and violation of privacy of individuals as a result of cybercrimes (Lin & Nomikos, 2018; Lintang et al., 2020). In this context, a few high profile cases can be cited. For example, a lecturer in a private university of Indonesia was convicted for violating Article 32 of the Electronic Information Law (Lubis et al., 2018; Manihuruk & Tarina, 2020; Thomas, 2013). The lecturer had edited an electronic document and the altered document was accessible to public as well. This crime is seen as a result of the weakness of the current harmonization of the cybercrime with the constitutional laws in Indonesia (Mansur & Gultom, 2005). In another example of 2013, a 19-year-old man was sentenced six-month imprisonment and a fine after being found guilty of trying to hack the official website of former president of Indonesia. In a similar case, another hacker faced a sentence of 15-month imprisonment after being found guilty of hacking the official website of Indonesian press council (Mansur & Gultom, 2005).

After analyzing these cases, books of laws should also be criticized for obvious lapses in cyber-security. The focus should be on the development of such a system that results in significant decrease of the crime itself. This can only be made possible with the help of complete harmonization of cybercrime with the constitutional law (Meinarni & Iswara, 2018; Moise, 2017). These cases are also examples of significant shortcomings and gaps in the current level of harmonization of cybercrime with the constitutional laws. It also reveals that there are no provisions for class actions over cyber security violations and data protection, as are available in other countries under environmental laws and consumer protection laws (Lubis et al., 2018; Manihuruk & Tarina, 2020; Thomas, 2013). It is also unknown whether there has ever been any significant attempt for filing a class action suit for violations against the cyber security and data protection in Indonesia (Lubis et al., 2018; Manihuruk & Tarina, 2020; Thomas, 2013).

Conclusion and recommendations

The current study observed and reviewed that cybercrime proving has been firmly regulated by various laws and regulations, in accordance with the positive law implemented in Indonesia, also known as the Indonesian Criminal Procedure Code, Act 19 of 2016 established vide decision of Constitutional Court Number 20/PUU-XIV/2016. The provisions related to cybercrime were first directly regulated in international regulations, under the 2001 convention on cybercrime organized by European Union. The European Council has worked for the overcoming of cybercrime in Indonesia without any kind of reduction in the opportunity for every member in the country to continue to develop various creative activities with the development of information technology. The law enforcement policies in Indonesia against the cybercrime are also carried out with the help of various penal and non-penal approaches. The penal approaches take the form of the criminalization for the purpose of streamlining positive laws that are related to cybercrime whereas the non-penal approaches take the form of approaches for the prevention of occurrence of cybercrimes. These involve enhancing the knowledge regarding these crimes for the law enforcement officers in relevance with the information and technology, enhancing the infrastructure and facilities, and improving efforts to improve the international cooperation.

The findings of the current study also revealed that the EIT law in Indonesia is significantly focused on electronic transactions and the content of electronic systems. Another law, GR Law 71/2019, has also made a significant focus on crimes which are purely related with the misuse of data, electronic transactions, spreading of the malicious codes and viruses and unauthorized electronic signatures. Thus bot the laws have a very limited and specific coverage, as they provide inadequate response to ever changing problems related to cybercrime and cyber threats specifically in the case of the critical infrastructure of the government. On the other side, the National Security, the Government, and the Ministry of Defense with its regulation No. 82/2014, have been working for national cyber security. These efforts however only focus on military cyber defense and tackle with only the cyber threats to national security. It is clear that these regulations do not cover nonmilitary cyber threats.

Considering these shortcomings and significant level of specific focus, there is a significant requirement for harmonization and consistency of cyber-security and cyber-laws. The existing regulations and policies for cyber security in Indonesia are fragmented across various ministries, according to which there is a lack of proper umbrella law that can provide a complete regulatory framework. There is a requirement of a coordinated and regulated sectoral system against cybercrime and cyber threats. In response to the enhancing cyber threats the government must pass a bill with the help of BSSN and the House of Representatives in order to provide with an umbrella framework which should consist of unified regulations and laws against cyber security in Indonesia. These unified and harmonized regulations and laws when regulated and harmonized with the constitutional law of Indonesia can provide unified and constant cyber security to every sector, corporation, individual and body in Indonesia against cybercrimes and threats.

References

Aditya, Z. F., & Al-Fatih, S. (2021). Indonesian constitutional rights: expressing and purposing opinions on the internet. *The International Journal of Human Rights, 25*(9), 1395-1419. https://doi.org/10.1080/13642987.2020.1826450

Altayar, M. S. (2017). A comparative study of anti-cybercrime laws in the Gulf Cooperation Council countries. *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)* (pp. 148–153). IEEE. https://doi.org/10.1109/Anti-Cybercrime.2017.7905281

Arief, B. N. (2006). *Tindak pidana mayantara: perkembangan kajian cyber crime di Indonesia.* Raja Grafindo Persada. http://library.stik-ptik.ac.id/detail?id=26459&lokasi=lokal

Azmi, R. H. N. (2020). Indonesian Cyber Law Formulation in The Development Of National Laws In 4.0 Era. *Lex Scientia Law Review, 4*(1), 46–58. https://doi.org/10.15294/lesrev.v4i1.38109

Broadhurst, R., & Chang, L. Y. (2013). Cybercrime in Asia: Trends and challenges. In *Handbook of Asian criminology* (pp. 49-63). Springer. https://doi.org/10.1007/978-1-4614-5218-8_4

Bryan, L. L. (2020). Effective information security strategies for small business. *International Journal of Cyber Criminology, 14*(1), 341-360. http://dx.doi.org/10.5281/zenodo.3760328

Bunga, D. (2019). Politik hukum pidana terhadap penanggulangan cybercrime. *Jurnal Legislasi Indonesia, 16*(1), 1–15. https://doi.org/10.54629/jli.v16i1.456

Chang, L.Y. (2020). Legislative Frameworks Against Cybercrime: The Budapest Convention and Asia. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 327-343. https://doi.org/10.1007/978-3-319-78440-3_6

Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015). *Cybercrime, digital forensics and jurisdiction.* Springer, Cham. https://doi.org/10.1007/978-3-319-15150-2

Choirunnisa, S. (2021). Legal Protection Against Women Victims of Sexual Harassment Through Social Media (Cyberporn). *The Indonesian Journal of International Clinical Legal Education, 3*(3), 367–380. https://doi.org/10.15294/ijicle.v3i3.48266

Christianto, H. (2020). Measuring cyber pornography based on Indonesian living law: A study of current lawfinding method. *International Journal of Law, Crime and Justice, 60*, 1-12. http://repository.ubaya.ac.id/id/eprint/37166

Dhanapal, S., Salman, N. W., Sabaruddin, J. S., & Nazeri, N. M. (2020). Criminalising Terrorism: An Overview of Malaysia's Anti-Terrorism Laws. *International Journal of Criminal Justice Sciences, 15*(1), 70-90. http://dx.doi.org/10.5281/zenodo.3821141

Djanggih, H. (2018a). The Phenomenon Of Cyber Crimes Which Impact Children As Victims In Indonesia. *Yuridika, 33*(2), 212-231. http://dx.doi.org/10.20473/ydk.v33i2.7536

Djanggih, H. (2018b). Urgency Legal Aspects Of Growth Information Technology In Indonesia. https://doi.org/10.31219/osf.io/h6vp8

Djanggih, H., Thalib, H., Baharuddin, H., Qamar, N., & Ahmar, A. S. (2018). The effectiveness of law enforcement on child protection for cybercrime victims in Indonesia. *Journal of Physics: Conference Series. 1028*(1) (pp. 012192). IOP Publishing. https://doi.org/10.1088/1742-6596/1028/1/012192

Dwipayana, N. L. A. M., Setiyono, S., & Pakpahan, H. (2020). Cyberbullying Di Media Sosial. *Bhirawa Law Journal, 1*(2), 63-70. https://doi.org/10.26905/blj.v1i2.5483

Ersya, M. P. (2017). Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. *Journal of Moral and Civic Education, 1*(1), 50-62. https://doi.org/10.24036/8851412020171112

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

Faiz, P. M. (2016). The Protection of Civil and Political Rights by the Constitutional Court of Indonesia. *Indonesia Law Review, 6*(2), 159-179. https://ssrn.com/abstract=2838900

Hakim, L., Kusumasari, T. F., & Lubis, M. (2018). Text mining of UU-ITE implementation in Indonesia. *Journal of Physics: Conference Series. 1007*(1) (pp. 012038). IOP Publishing. https://doi.org/10.1088/1742-6596/1007/1/012038

Hatta, M. (2020). The Spread of Hoaxes and Its Legal Consequences. *International Journal of Psychosocial Rehabilitation, 24*(03), 1750-1760. http://repository.unimal.ac.id/id/eprint/5338

Hermawan, R. (2015). Kesiapan Aparatur Pemerintah dalam Menghadapi Cyber Crime di Indonesia. *Faktor Exacta, 6*(1), 43-50. http://dx.doi.org/10.30998/faktorexacta.v6i1.217

Indrajit, R. E. (2016). Keamanan Informasi dan Internet. *Seri Bunga Rampai Pemikiran Ekoji.* https://www.academia.edu/download/38303226/pr241-KeamananInformasi-Sosialisasi-Ambon-IDSIRTII.ppt.pdf

Jaelani, A. K., & Luthviati, R. D. (2021). The Crime Of Damage After the Constitutional Court's Decision Number 76/PUU-XV/2017. *Journal of Human Rights, Culture and Legal System, 1*(1), 31-42. https://doi.org/10.53955/jhcls.v1i1.5

Jang, Y. J. (2013). Harmonization among national cyber security and cybercrime response organizations: new challenges of cybercrime. *arXiv preprint arXiv:1308.2362*, 1-15. https://arxiv.org/ftp/arxiv/papers/1308/1308.2362.pdf

Karo, R. K., & Sebastian, A. (2019). Juridical Analysis on the Criminal Act of Online Shop Fraud in Indonesia. *Lentera Hukum, 6*(1), 1-14. https://doi.org/10.19184/ejlh.v6i1.9567

Krysiński, D., & Szczepański, J. (2020). Continuity and contestation. Structural and cultural background of transportation preferences in Poland. *socialspacejournal.eu, 19*(1), 111-141. http://mail.socialspacejournal.eu/Social%20Space%20Journal%2012020(19).pdf#page=111

Kshetri, N. (2013). *Cybercrime and cybersecurity in the global south.* Springer. https://doi.org/10.1057/9781137021946

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security, 45*, 58-74. https://doi.org/10.1016/j.cose.2014.05.006

Laurensius, S., Situngkir, D., Putri, R., & Fauzi, R. (2018). Cyber Bullying Against Children In Indonesia. *International Conference on Social Sciences, Humanities, Economics and Law*. European Alliance for Innovation (EAI). http://dx.doi.org/10.4108/eai.5-9-2018.2281372

Lim, M. (2013). The internet and everyday life in Indonesia: A new moral panic? *Bijdragen tot de taal-, land-en volkenkunde/Journal of the Humanities and Social Sciences of Southeast Asia, 169*(1), 133-147. https://doi.org/10.1163/22134379-12340008

Lin, L. S., & Nomikos, J. (2018). Cybercrime in East and Southeast Asia: The Case of Taiwan. In *Asia-Pacific Security Challenges* (pp. 65-84). Springer. https://doi.org/10.1007/978-3-319-61729-9_4

Lintang, L. C., Martufi, A., & Ouwerker, J. (2020). The Alternative Concepts of Blasphemy Law in Indonesia: Legal Comparison with Ireland and Canada. *BESTUUR, 9*(1), 13-25. https://doi.org/10.20961/bestuur.v9i1.51632

Lubis, M., Kusumasari, T. F., & Hakim, L. (2018). The Indonesia Public Information Disclosure Act (UU-KIP): Its Challenges and Responses. *International Journal of Electrical & Computer Engineering, 8*(1), 94-103. http://doi.org/10.11591/ijece.v8i1

Manihuruk, H., & Tarina, D. D. Y. (2020). State Defense Efforts through Strengthening Cyber Law in Dealing with Hoax News. *International Journal of Multicultural and Multireligious Understanding, 7*(5), 27-36. http://dx.doi.org/10.18415/ijmmu.v7i5.1590

Mansur, D. M. A., & Gultom, E. (2005). *Cyber Law-Legal Aspects of Information Technology*. Refika Aditama.

Maskun, M., Nugraha, R., Assidiq, H., Tayyib, M., & Syafira, A. (2021). Harmonization Over the Regulations of Electronic Medical Records and its Potential to be Abused. *Medico-legal Update, 21*(1), 1760-1765. http://repository.unhas.ac.id/id/eprint/5126

Meinarni, N. P. S., & Iswara, I. B. A. I. (2018). Hoax and its Mechanism in Indonesia. *Proceedings of the International Conference of Communication Science Research (ICCSR 2018)* (pp. 183-186). Atlantis Press. https://doi.org/10.2991/iccsr-18.2018.39

Moise, A. C. (2017). The Legal Regulation of Cybercrime in the United States of America Legislation. *Journal of Advanced Research in Law and Economics (JARLE), 8*(27), 1576-1578. https://www.ceeol.com/search/article-detail?id=607305

Mulyadi, M. (2008). *Criminal Policy: Pendekatan Integral Penal Policy dan Non Penal Policy dalam Penanggulangan Kejahatan Kekerasan*. Pustaka Bangsa Perss.

Muthia, F. R., & Arifin, R. (2019). Kajian Hukum Pidana Pada Kasus Kejahatan Mayantara (Cybercrime) Dalam Perkara Pencemaran Nama Baik Di Indonesia. *RESAM Jurnal Hukum, 5*(1), 21-39. https://doi.org/10.32661/resam.v5i1.18

Naro, W., Syatar, A., Amiruddin, M. M., Haq, I., Abubakar, A., & Risal, C. (2020). Shariah Assessment Toward the Prosecution of Cybercrime in Indonesia. *International Journal of Criminology and Sociology, 9*, 572-586. http://repositori.uin-alauddin.ac.id/id/eprint/17812

Nurahman, D. (2020). Cybercrime Policies: Juridical Evidence and Law Enforcement Policies. *Proceedings of The International Conference on Environmental and Technology of Law, Business and Education on Post Covid 19*. EAI. http://dx.doi.org/10.4108/eai.26-9-2020.2302579

Prahassacitta, V. (2016). The Concept of Extraordinary Crime in Indonesia Legal System: is The Concept An Effective Criminal Policy? *Humaniora, 7*(4), 513-521. https://doi.org/10.21512/humaniora.v7i4.3604

Prayudi, Y., Ashari, A., & Priyambodo, T. K. (2015). A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia. *International Journal of Computer Network and Information Security, 7*(11), 1-8. https://doi.org/10.5815/ijcnis.2015.11.01

Rahmawati, I. (2017). the Analysis Ofcyber Crime Threat Risk Management To Increase Cyber Defense. *Jurnal Pertahanan & Bela Negara, 7*(2), 37-52. http://dx.doi.org/10.33172/jpbh.v7i2.193

Salavrakos, I.-D. (2020). A Re-Assessment of Italian Defence Production and Military Performance in the World Wars. *Res Militaris, 10*(1). https://resmilitaris.net/index.php/2020/01/01/id1031542/

Saputra, R. W. (2016). A survey of cyber crime in Indonesia. *2016 International Conference on ICT For Smart Society (ICISS)* (pp. 1-5). IEEE. https://doi.org/10.1109/ICTSS.2016.7792846

Schjolberg, S. (2008). The history of global harmonization on cybercrime legislation–the road to geneva. *Journal of international commercial law and technology, 1*(12), 1-19. https://www.cybercrimelaw.net/documents/cybercrime_history.pdf

Setiadi, F., Sucahyo, Y. G., & Hasibuan, Z. A. (2012). An overview of the development indonesia national cyber security. *International Journal of Information & Computer Science, 6*, 106-114. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.394.3095&rep=rep1&type=pdf

Smith, R., & Perry, M. (2021). Fake news and the convention on cybercrime. *Athens Journal of Law, 7*(3), 335-358. https://ssrn.com/abstract=3878059

Suhariyanto, B. (2014). *Information Technology Crime (CYBERCRIME)*.

Sunkpho, J., Ramjan, S., & Ottamakorn, C. (2018). Cybersecurity policy in ASEAN countries. *17th Annual Security Conference* (pp. 1-7). Information Institute Conferences. https://www.researchgate.net/publication/324106226

Tapsell, R. (2019). Indonesia's policing of hoax news increasingly politicised. *Yusof Ishak Institute, ISEAS PERSPEVTIVE*(75), 1-10. https://www.iseas.edu.sg/images/pdf/ISEAS_Perspective_2019_75.pdf

Thomas, D. (2013). *Cybercrime: Security and Surveillance in the Information Age* (1st Edition ed.). Routledge. https://doi.org/10.4324/9780203354643

Tosoni, L. (2018). Rethinking Privacy in the Council of Europe's Convention on Cybercrime. *Computer Law & Security Review, 34*(6), 1197-1214. https://doi.org/10.1016/j.clsr.2018.08.004

Ulima, D. T. (2018). The Criminal Liability of The Defamation Perpetrators Against The President or Vice President After Having The Court Decision Number Constitutional 013-022/Puu-Iv/2006. *YURISDIKSI: Jurnal Wacana Hukum Dan Sains, 11*(2), 46-63. https://yurisdiksi.unmerbaya.ac.id/index.php/yurisdiksi/article/view/22

Wahid, A., & Labib, M. (2005). Crimes of Mayantara. In. Bandung: Refika Aditama.

Wahid, A., & Labib, M. (2005). *Mayantara Criminal, Bandung, Refika Aditama Bambang Poernomo.*

Wild, C., Weinstein, S., MacEwan, N., & Geach, N. (2011). *Electronic and Mobile Commerce Law: An Analysis of Trade, Finance, Media and Cybercrime in the Digital Age.* University of Hertfordshire Press. https://books.google.com/books?id=Y6LHR9dS2XwC

Yusa, G. (2017). The Authority of Government in Clearing Hatefull and Hostilities. *International Journal of Electrical and Computer Engineering (IJECE), 7*(6), 3735-3744. http://doi.org/10.11591/ijece.v7i6.pp3735-3744

Zulfikar, A., Sukananda, S., Baharuddin, H., & Sampara, S. (2020). Harmonization of International Law in Indonesian Legal System: The Study of Indonesian Migrant Workers Protection Overseas. *LawArXiv*, 1-17. https://doi.org/10.31228/osf.io/g5kqw