Harmonization of Cybercrime Arrangements in Criminal Law

Agus Salim¹, Karel Roni Pakambanan², Liberthin Palullungan³
Departement of Law, Universitas Kristen Indonesia Paulus (UKIP)
Makassar, Indonesia¹,²,³

Abstract-This article presents the harmonization of cybercrime arrangements in criminal law. Harmonization of cybercrime arrangements in criminal law is carried out by harmonizing the substance of criminal acts both internal harmonization, namely harmonization between the Criminal Code as general rules and legislation outside the Criminal Code as special rules, as well as external harmonization, namely harmonization of the Criminal Code with regional and international provisions in the field of Cybercrime. In addition it is necessary to harmonize the policy formulation on cybercrime in an integrated manner in the Criminal Code or formulated in a special law and the urgency of harmonizing criminal provisions in the field of information technology is to create criminal provisions in accordance with the characteristics of crimes in the field of information technology perpetrators of crimes in the field of information technology, victims crimes in the field of information technology, and Indonesian society along with their values of wisdom and expected norms in the provisions of law and the international community.

Keywords: Harmonization; Arrangement; Cybercrime; Criminal law

Introduction

Cybercrime first occurred in America in the 1960s [1]. Cybercrime covers a very broad understanding, namely computer crime, internet crime, including activities that use computers as a means of committing the crime. Therefore, cybercrime needs to be regulated by cybercrime law to create legal certainty in society. Cybercrime law (in the sense of material) in Indonesia is contained in the Criminal Code and criminal provisions outside the Criminal Code, because the Criminal Code is part of criminal law.

General provisions governing the application of criminal law are in Book I of the Criminal Code (General Rules), so that if no other provisions are specified, then the principles of the Criminal Code can be applied to all criminal provisions in Indonesia. If a statutory regulation regulates the deviations of the principles in the Criminal Code Book I, the provisions are considered invalid, except for the deviant laws and regulations in the form of Laws (Special Rules). The effectiveness of this provision is based on the principle "special provisions override general provisions" (lex specialist derogate legi general) [2].

Based on Book 1 of the Criminal Code, the jurisdiction of the application of criminal law includes the enforcement of criminal law according to time, and the validity of criminal law according to place. Since 1983, courts in Indonesia have tried cybercrime cases based on the provisions of the Criminal Code by making extensive interpretations of the provisions contained in the Criminal Code.

Based on UU-ITE, Article 1 number 3, namely Law number 11 the Year 2008 which has been amended by Law number 19 the Year 2016 explains the notion of Information Technology is a technique for collecting, preparing, storing, processing, announcing, analyzing, and/or disseminating information. In the legal context in the field of information technology, understanding of information technology leads to the use of computer-based information and communication technology.

In the context of criminal law in the field of information technology, the scope of criminal law in the field of information technology includes the notion of criminal law in the broadest sense, namely;
a. Material criminal law (including provisions of the Criminal Code (KUHP) and Criminal Law propositions in statutory regulations) outside the Criminal Code (for example in the ITE Law, the Pornography Law, the Communication Law, the Copyright Law),

b. Formal criminal law (consisting of provisions in the Criminal Procedure Code (KUHAP) and criminal procedural law provisions that are outside the Criminal Procedure Code (eg UU-ITE, Pornography Law, Communication Law, Copyright Law), and

c. Panitensier law (consisting of criminal provisions both in Book I of the Criminal Code, and other provisions that are spread outside Book I of the Criminal Code, for example in RI Law Number 20 of 1946 concerning Penalty Closing, Law Number 12 of 1995 concerning Corrections, Law Number 11 of Year 2012 concerning the Juvenile Justice System, and its implementing laws and regulations.

Information technology is now a double-edged sword because, in addition to contributing to the improvement of human welfare, progress and civilization, it is also an effective means of acting against the law. Vol. 3. No. 1 2018 against the law [3]. According to Barda Nawawi Arief, cybercrime is one of the new forms or dimensions of contemporary crime that is gaining widespread international attention. Furthermore, Barda Nawawi Arief said that in the perspective of criminal law, efforts to counter cybercrime can be seen from various aspects, including aspects of criminalization policy (formulation of criminal acts), aspects of criminal liability or punishment (including aspects of evidence / 3 pieces of evidence), and aspects of jurisdiction [4].

According to its nature Cybercrime is included in the category of borderless crime (crimes without space and time restrictions), so in combating cybercrime crime, complex, integrated and continuous steps from many parties are required, not just law enforcement duties [5]. Based on the identification of the Association of Indonesian Internet Service Managers (APJII), the form and number of cybercrime in Indonesia from 2001 to 2005 that the largest number of cybercrime in Indonesia occurred in 2003 which was 12,976 cases, then the least number of cases in 2002, namely 183 cases. The most common form of crime is spam or junk mail or "junk e-mail", which is 12,396 cases (58.89%) [6].

Provisions in the Criminal Code, used to deal with cybercrime are provisions regarding counterfeiting (Articles 263-276), theft (Articles 362-367), fraud (378-395), destruction of goods (Articles 407-412). While the provisions of the legislation outside the KUHP that can be used in dealing with cybercrime, among others, as follows:


b. RI Law number 10 of 1995 concerning customs as amended through RI number Law 17 of 2006 concerning amendment to Law number 10 of 1995 concerning customs.


d. RI Law number 19 of 2002 concerning copyright.

e. RI Law number 10 of 1998 concerning banking.

f. RI Law number 5 of 1999 concerning business competition.

g. RI Law number 36 of 1999 concerning telecommunications.

h. RI Law number 32 of 2002 concerning broadcasting

i. RI Law number 15 of 2003 concerning the stipulation of government regulations instead of Law number 1 of 2002 concerning eradication of the criminal acts of terrorism into Laws.

j. RI Law number 15 of 2002 concerning money laundering.

k. RI Law number 8 of 2010 concerning prevention and eradication of money laundering crimes.

l. RI Law number 21 of 2007 concerning eradication of trafficking in persons.

m. RI Law number 11 of 2008 concerning electronic information and transactions.
Research Method
The type of research used in this study is the normative juridical type of research that is research conducted qualitatively by relying on library studies. Within library research data and information can be obtained following the principles of rational, critical, objective, both originating from primary, secondary, and tertiary legal material.

Results And Discussion
3.1 Harmonization Of Material Or Substance Of Criminal Acts
There are 2 types of harmonization of cybercrime in criminal law, namely internal harmonization and external harmonization.

3.1.1 Internal harmonization (national harmonization) in Indonesia does not need to be done. The Draft of Criminal Code, does not need to be carried out, in harmony with the laws and regulations in Indonesia, for example concerning crimes in the field of telecommunications, money laundering, corruption, banking, copyrights. This is based on the idea that in the criminal legal system, the position of the Criminal Code as the main criminal law (general rules), while other laws or criminal provisions in the legislation outside the Criminal Code, are special rules. Legislation that regulates criminal acts outside the Criminal Code needs to harmonize with the substance of the Criminal Code, especially Book I.

3.1.2 External harmonization (regional harmonization or international harmonization or global harmonization) has been carried out by the drafter of the Criminal Code. This can be seen from the pouring of several provisions of the Convention on Cybercrime in the Indonesian Criminal Code Bill in 2010. Criminalization policy in the field of cybercrime is not merely a matter of national policy but also related to regional and international policies. For this reason, the Criminal Code Bill has harmonized with the provisions of the Convention on Cybercrime and criminal law abroad. Harmonization carried out in the Criminal Code Bill is in line with the UN's appeal through the United Nations International Review of Criminal Policy Manual on The Prevention and Control of Computer-Related Crime. This is in line with what Sunaryati Hartono said, that the harmonization of Indonesian law with international law needs to be done [7]

3.2 Harmonization Of Formulation Policies Against Cybercrime
The study in the field of formulation policy harmonization focuses on the issue of whether the formulation policy or cybercrime legislation in Indonesia is formulated in a specific law or integrated into the Criminal Code. Harmonization of this substantive formulating policy is highly dependent on the material criminal law system that already exists and will be built in Indonesia. This is intended so that the newly formed law is in one criminal law system in Indonesia. Material criminal law in force in Indonesia currently consists of the entire system of statutory rules in the Criminal Code (as a master rule or general rule), and specific criminal provisions outside the Criminal Code.

Material criminal law in force in Indonesia currently consists of the entire system of statutory rules in the Criminal Code (as a master rule or general rule), and specific criminal provisions outside the Criminal Code.
Theoretically, there are 2 models of pouring laws and regulations that can be used to regulate cybercrime, namely the umbrella provision model and the triangle regulation model.

3.2.1 Model Provisions Umbrellas (Umbrella Provision)
The umbrella regulation model is implemented by first making a "legal umbrella" in the form of the "Umbrella Law" concerning cybercrime law. After that, the legislator makes legislative regulations (implementing regulations) that are hierarchically equivalent to or lower than the "Umbrella Law". The law which is used as a "legal umbrella" only contains provisions that are taking into account all interests. The advantage of this model is that the Act can accommodate several provisions regarding internet technology (cyberspace) that are developing rapidly. Besides, this regulation can be more complete because it is regulated in several laws to guarantee legal certainty.
3.2.2 Triangle Regulation Model

The casting with the Triangle Regulation model focuses more on the problem which objects should be prioritized to be arranged in advance in detail. The laws and regulations which must be issued first to regulate cyberspace are as follows:

a. Regulations on Electronic Transactions (E-Commerce) or Online Transactions which regulate digital signatures and certification of authority, aspects of proof of electronic evidence, consumer protection, antitrust and unfair competition, taxation, and insurance.

b. Regulations on privacy protection for business people and consumers, which include electronic database protection, individual/company records.

c. Cybercrime arrangements, which include the jurisdiction and competence of the judiciary for cases that occur in cyberspace, such as fraud through computers or through telecommunications networks, threats and extortion, libel, sexual exploitation of children, and other substances not worth transmitting over the internet.

Based on the two pouring models mentioned above, then cybercrime in Indonesia is regulated by the umbrella provisions model, namely in the upcoming Criminal Code (as the Umbrella Law). While other provisions that can support the implementation of the Criminal Code are regulated in other specific Acts (implementing regulation). If this is not possible, implementing regulations can be contained in a Government Regulation (PP) or Presidential Regulation (Perpres).

3.3 Urgency Of Harmonization Of Criminal Provisions In Information Technology In Indonesia

Harmonization of law is an effort to analyze several legal norms so that one does not conflict with one another. The thought of harmonization stems from Rudolf Stammler who argues that the concept and principles of just law include harmonization (compatibility) between the "aims, objectives and interests of individuals" with "the aims, objectives and interests of the general public." There are 2 main ideas can be used as a basis for legislators in harmonizing cybercrime provisions in Indonesia, namely:

3.3.1. Harmonization of Material or Substance of Criminal Acts

In the study of the cybercrime law, it is necessary to involve experts in the field of information technology, because they know more about the actions that are considered harmful and most dangerous for the community. The recommended actions should be criminalized. Besides, it is also necessary to have input from various groups regarding legal interests or what values should be protected from the negative influence of misuse of information technology in cyberspace. If the identification of acts based on the scientific discipline of information technology is sufficient, then legal experts will formulate the construction of criminal acts and sanctions in a legal norm then pour them in an academic draft. In drafting the draft it is necessary to pay attention to the conceptions and theories of criminalization, penalization, and harmonization from the perspective of criminal science.

Concerning material harmonization, there are two studies of harmonization, namely internal harmonization and external harmonization.

a. Internal harmonization (national harmonization) is a study of harmonization or synchronization of the substance of criminal acts and sanctions to be regulated, with criminal acts and sanctions that already exist or have been regulated in positive law in Indonesia.

b. External harmonization (regional harmonization or international harmonization or global harmonization) is a study of the harmonization of criminal acts and sanctions to be made, with the legal substance governing cybercrime that is agreed internationally or globally or regionally. For example the harmonization of criminal provisions relating to computers in Indonesia with the Convention on Cybercrime, and the results of the UN Congress, as well as the work of the OECD and the European Council.

3.3.2 Harmonization of Cybercrime Formulation Policies

The study in the area of harmonization focuses on whether the policy formulation or criminal act legislation in the cyber field is included in a special law or integrated into a generally applicable law (KUHP). Harmonization of the formulative policy of substantive law is highly dependent on the material criminal law system that already exists or is to be built. It is intended that the new law is in one existing
system in Indonesia. Material criminal law in force in Indonesia currently consists of the entire system of statutory rules (statutory rules) that exist in the Criminal Code (as the main general rule), and criminal law outside the Criminal Code. In the Criminal Code consists of general rules, namely in Book I, and special rules, namely in Book II and Book III. Also, special rules also exist in criminal laws that are spread outside the Criminal Code.

The descriptions above are in line with the efforts to overcome cybercrime, which was formulated by the UN Congress in a Workshop on computer-related crime, in April 2000. In the congress, it was stated explicitly that "States should seek harmonization on the relevant provisions in criminalization, evidence and procedure."[8]. Countries need to harmonize the provisions relating to criminalization, verification and procedure of criminal proceedings in court based on applicable law because the government is the personification of the State to perform the tasks determined by law [9]. The benefit of harmonization is that criminal provisions are obtained following the characteristics of crimes in the field of information technology, perpetrators of crimes in the field of information technology, victims of crimes in the field of information technology, and the people of Indonesia and their values of wisdom. Besides, through harmonization, norms in criminal provisions will be appropriate.

Conclusion

1. Harmonization of Cybercrime arrangements in criminal law is carried out by harmonizing the substance of criminal acts both internal harmonization, namely harmonization between the Criminal Code as general rules and legislation outside the Criminal Code as special rules, as well as external harmonization, namely the harmonization of the Criminal Code with regional and international provisions in the field of Cybercrime. Also, it is necessary to harmonize policy formulation on cybercrime in an integrated manner in the Criminal Code or formulated in a special law.

2. The urgency of harmonizing criminal provisions in information technology is to create criminal provisions in accordance with the characteristics of crimes in the field of information technology perpetrators in the field of information technology, victims of crimes in the field of information technology, and Indonesian society along with their values of wisdom and expected norms in legal provisions and the international community.

Acknowledgment

The author would like to state appreciations to the Universitas Kristen Indonesia Paulus (UKI-Paulus) in Makassar, Indonesia for supporting to publish this article

References


[10] Republic of Indonesia Law Number 11 Year 2008 Regarding Information and Electronic Transactions

*Corresponding Author: Agus Salim, Email: agus.salim@ukipaulus.ac.id
Article History: Received: Sep 02, 2019, Accepted:Nov 28, 2019