International Conference Restructuring and
Transforming Law 2025
Volume 4, Issue 1, July 2025
e-ISSN : 2963-931X
icrtlaw@ums.ac.id

CYBER LAW: PROTECTION OF SOCIETY FROM CYBER CRIME IN A PROPHETIC PERSPECTIVE

Arum Dwi Arta Setyoningsih
Universitas Muhammadiyah Surakarta
C100210002@student.ums.ac.id

Achmad Miftah Farid
Universitas Muhammadiyah Surakarta
amf209@ums.ac.id

Abstract

Introduction: The role of law enforcement officers as regulated in Law Number 19 of 2016 concerning Amendments to the ITE Law and Law Number 1 of 2024 concerning the Second Amendment to the ITE Law is crucial in efforts to eradicate cybercrime. Their responsibilities include detection, investigation, prosecution of cybercriminals, as well as prevention and handling of cyberattacks. In addition to positive law in Indonesia, cybercrime can also be viewed from a prophetic law perspective. Method: This study uses a normative or doctrinal method with primary data in the form of literature. This type of research is descriptive in nature which aims to provide a representative picture of cyber law and community protection in prophetic law. The approaches used are philosophical, legislative, and literature approaches. Results and Discussion: From the results of the study, it is understood that cybercrime is a form of crime that has emerged in the modern era. According to the analysis of Islamic law (jinayat), perpetrators of cybercrime can be subject to ta'zir punishment. Ta'zir linguistically means prevention (al-man'u). In sharia terminology, ta'zir is an educational punishment (ta'dib) determined based on sin. The punishment can vary from light to severe according to the level of danger.

Keywords: Cybercrime, Prophetic, Perspective, Islam

INTRODUCTION

In terminology, crimes in the field of computer-based information technology such as those that occur today can be called by several terms, such as computer misuse, computer fraud, computer-related crime, or computer crime. Cybercrime is an illegal act with or without damaging a computer system that is used as a means or target of crime (2).

Cyber law is a law that regulates activities in cyberspace (cybercrime via the internet network) (3). This term forms a new legal regime in Indonesia, especially in technology and information activities

(4). The cyber legal regime in Indonesia is marked by the birth of Law (5). Cyber law is needed because cyber activities are not limited by state territory and can be done at any time. Although the evidence is virtual and electronic, the impact is real (6).

In Indonesian law, cybercrime is regulated in Law Number 11 of 2008 concerning Information and Electronic Transactions which has been amended by Law Number 19 of 2016 concerning Information and Electronic Transactions and in Law Number 36 of 1999 concerning Telecommunications. In the Law on Information and Electronic Transactions related to cybercrime can be seen in Article 27 paragraph (1) to paragraph (3) and Article 30: (1) Any person intentionally and without the right distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents containing content that violates morality; (2) Any person intentionally and without the right distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents containing gambling content; and (3) Any person intentionally and without the right distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents containing insulting and/or defamatory content.

Article 27 paragraph (1) explains about morality, Article 27 paragraph (2) explains about gambling and Article 27 paragraph (3) about insults and/or defamation. Based on Article 30 paragraphs (1) to (3) which read: (1) Any person who intentionally and without rights or against the law accesses another person's Computer and/or Electronic System in any way; (2) Any person who intentionally and without rights or against the law accesses a Computer and/or Electronic System in any way with the aim of obtaining Electronic Information and/or Electronic Documents; and (3) Any person who intentionally and without rights or against the law accesses a Computer and/or Electronic System in any way by violating, breaking through, exceeding, or breaking the security system (7).

Article 30 explains about unauthorized access to computers and/or electronic systems belonging to others. In Law Number 36 of 1999 concerning Telecommunications related to cybercrime, there is Article 22. This article provides a criminal threat to anyone who violates the provisions of the law. Article 22 states that "Everyone is prohibited from carrying out acts without rights, unlawfully, or manipulating telecommunications network access; and/or telecommunications service access; and/or special telecommunications network access" (8).

Cybercrime cases are increasing every year along with the rapid development of digital technology. Law enforcement faces challenges such as lack of understanding by officers and the need for more comprehensive criminal policies to protect victims and prevent further crimes.

In a prophetic perspective, Allah SWT limits human behavior in order to uphold justice, order, and peace in society, so that the purpose of life can be achieved, including the protection of human souls. This perspective views that maintaining public order is more important than personal interests. Therefore, actions such as cybercrime are categorized as violations of the law.

Legal research method is a process to find a legal rule, legal principle, or legal doctrine to answer the legal problems faced. The research method used is normative research, namely to find legal norms, principles, or legal doctrines to answer the legal problems faced. The type of research is descriptive, with an approach to legal theory, legislation, and analyzed philosophically to reveal the ontological and philosophical basis of legal protection in a prophetic perspective.

METHOD

This research method is a normative or doctrinal method where the research used is library research, namely research with primary data is library data where the author collects and examines archives or literature studies such as books, papers, articles, journals, or others (9). With the aim of obtaining the necessary data by studying and citing data obtained from books or decisions regarding cybercrime in Indonesia, a philosophical approach and a legislative approach are carried out by examining all laws and regulations related to cybercrime and cyber law which are handled and analyzed with philosophical analysis so that the ratio legis, ontological basis and philosophical basis of protection regulations in a prophetic perspective can be known.

RESULT AND DISCUSSION

Cybercrime is divided into two categories, namely cybercrime in the narrow sense and in the broad sense. Cybercrime in the narrow sense is a crime against a computer system, while in the broad sense it includes crimes against a computer system or network, as well as crimes that use computer facilities as a means (10).

Some literature on cybercrime is identified as a computer crime. According to the US Department of Justice, a computer crime is: “Any illegal act that requires knowledge of computer technology to commit, investigate, or prosecute.”

Another opinion was put forward by the Organization for Economic Cooperation Development (OECD) which uses the term computer related crime which means: "Any illegal, unethical or unauthorized behavior involving automated data processing and/or data transmission." Several definitions of computer crime can be formulated that computer crime is an unlawful act carried out using a computer as a means/tool or a computer as an object, whether to gain profit or not, thereby harming another party (11).

Based on the rapid development of telematics (internet) which is directly proportional to the emergence of crime modes. Several years ago, tens of thousands of internet users were attacked by the e-mail virus "melissa" and "ex-plore.zip.worm" which spread quickly, deleting

archives, requiring systems, and causing companies to have to spend millions of dollars to get help and deadlines (12).

In February 2000, for example, some of the most popular consumer and commercial networks such as Yahoo, Amazon, eBay, CNN.com, and E-trade were shut down by crackers who sent so many messages that the networks became overloaded. In addition, other networks have been the target of pagejacking, which connects users to unwanted networks (11).

Based on the description above, it can be concluded that the scope of cybercrime is: piracy, fraud, theft, pornography, harassment, slander and forgery (11). From the definition and types of cybercrime above, cybercrime is one form of crime that has emerged in the modern era today. Thus, cybercrime according to Islamic law analysis (jinayat) can be punished with ta'zir. Ta'zir according to the meaning of language means prevention (al-man'u). According to the term ta'zir is an educational punishment (ta'dîb) in the sense of anticipating by intimidating (tankîf). According to sharia, ta'zir is intended as a sanction imposed on the basis of disobedience, because it is expressly not included in the crimes contained in the Qur'an and Hadith, such as had, qisas, or kafârat (13).

Cybercrime is a criminal activity that uses computer facilities or computer networks without permission and against the law, either by changing or not changing (damaging) the computer facilities that are entered or used or crimes that use electronic media such as the internet because it is categorized as cybercrime, or crimes in the computer field in unlawful ways (2). It can also be categorized as computer crimes aimed at a computer system or network, which includes all forms of new crimes that use the help of electronic media internet. The sanctions for perpetrators of cybercrime according to Islamic law are ta'zir through a trial process with a judge's decision with the threat of punishment in the form of imprisonment, exile, flogging, up to the death penalty according to the level of loss that has been committed.

From a prophetic perspective, the punishment for cybercrime perpetrators varies. According to a prophetic perspective, cybercrime (jinayat and jarimah) can be punished with ta'zir. Ta'zir according to the meaning of language means prevention (al-man'u). According to the term ta'zir is an educational punishment (ta'dib) in the sense of anticipating by intimidating (tankif). According to sharia, ta'zir is intended as a sanction imposed on the basis of disobedience, because it is expressly not included in the crimes contained in the Qur'an and Hadith, such as had, qisas, or kafarat (14).

Similarities and differences regarding cybercrime and jinayah jurisprudence (15):

1. Unauthorized access to computer systems and services with sharia (theft):

*Sharia*namely the act of taking goods or something belonging to another person without permission secretly from the storage place to control the goods. The similarity between unauthorized access to computer systems and services with sharia (theft) is that both are stealing.

Unauthorized access to computer systems and services occurs in cyberspace including carding (sabotaging other people's credit cards and spending them illegally). While sharia is in the real world. In unauthorized access to computer systems and services, what is taken is data, while in sharia what is taken is money or goods. The perpetrators of unauthorized access to computer systems and services are called hackers, while the perpetrators of sharia are called thieves.

1. Illegal content and kadzib (lies)
2. *Kadzib*is an act of lying, namely an act that is not in accordance with the words of conscience and the actual reality. The similarity between illegal content and kadzib (lies) is that both are lies.
3. Illegal content exists in cyberspace which is often called hoax while kadzib occurs in the real world. Hoax is an act of spreading false and misleading news which can be categorized as fraud. Sometimes the hoax news is intended to embarrass someone so it is often called cyber bullying (behavior that lowers the self-esteem and mentality of others). While kajib is often interpreted as a lie (16).

2. Data falsification and altazif (forgery)

*Altarif*is the act of falsifying goods or documents to deceive others, such as fake letters that can give rise to rights, obligations, or debt relief, and so on. The similarity between data falsification and altazif is that both commit falsification.

Data falsification occurs in cyberspace, while altazif occurs in the real world, such as perjury, false witness, or document falsification by adding or reducing documents.

3. Cyber espionage and spying (tajasus)

*Tajasus*is the act of spying or finding out about something secretly. The similarity between cyber espionage and tajasus is that both involve spying.

Cyber espionage that occurs on the internet can be aimed at imitation (copying) products or finding weaknesses in business competitors so that they experience decline (bankruptcy). While tajasus occurs in the real world.

4. Cyber terrorism and tahdid (threat)

*Tahdid*is an act of threatening or intimidating someone so that the victim feels uncomfortable or afraid. The similarity between cyber terrorism and tahdid is that both are equally threatening.

The threat of cyber terrorism is carried out subtly by a hacker (a person who has expertise in computer programming who likes to tinker with other people's computer programs. Whereas tahdid is carried out openly.

5. Criminal acts against intellectual property and other things (plagiarism or manipulation)

*Alaintihal*is the act of taking someone else's work and then making it look like it is your own work or plagiarizing someone else's written work. There is also the term aintihal alhuia (fraud or imitation), which is an act of deception to gain personal gain at the expense of others. The similarity between criminal acts against intellectual property and alaintihal is that both are imitating each other.

The crime of intellectual property is claiming someone else's property as one's own via the internet, while the crime of claiming someone else's property as one's own property is essentially an object.

6. Violation of privacy and hirabah (usurpation)

*Hirabah*namely the act of taking property or transferring ownership rights to another person's property through unlawful transactions accompanied by coercion. The similarity between invasion of privacy and hirabah is that both take other people's property and both disturb (disrupt) public security.

Privacy violation is a way of robbing in a wise way via the internet, while hirabah still uses the old way, namely face to face between the perpetrator and the victim.

*Ta'zir*prophetically intended as a sanction imposed on the basis of disobedience, because it explicitly does not include criminal acts contained in the Qur'an and Hadith, such as hadd, qisas, or kafârat (14). Although ta'zir punishment is a lesson for the perpetrator, ta'zir punishment

varies from the lightest to the most severe according to the level of crime committed by the perpetrator. In the book Al-Fiqh 'Ala Al-Madzahib Al-'Arba'ah Abdurrahman Al-Jaziri mentions several types of ta'zir punishment as follows (15):

The punishments in question are tahdid (threat), tanbih (reprimand), and al-Wadh'u (warning).

There is no specific punishment for perpetrators of cyber espionage (spying), so the judge can impose a sentence of tahdid, tanbih, or al-Wadh'u on the perpetrator.

1. Excommunication penalty: Regarding criminal acts of intellectual property (hoaxes), the punishment for the perpetrators is not explained, so the judge can impose a penalty of excommunication or social sanctions in the form of an appeal for the person concerned to be shunned by society.
2. Fines: Regarding intellectual property crimes (plagiarism), the punishment for the perpetrator is not explained, so the judge can impose a fine according to the extent of the loss suffered by the victim.
3. Caning punishment: Regarding the crime of cyber data falsification, the punishment is 100 lashes and exile for 1 year.
4. Prison sentences: Regarding intellectual property crimes (fraud), the punishment for the perpetrator is not explained, so the judge can impose a prison sentence.
5. Exile sentence: Regarding the crime of cyber data falsification, Caliph Umar bin Khattab once sentenced the perpetrator of the Baitul Mal stamp to 1 year of exile and 100 lashes.
6. Death penalty: Cyber terrorism (threats) and violation of privacy (robbery) that disturbs public order are punishable by death.

Cybercrime from a prophetic perspective can be classified as jarimah, namely an act that contains sin or crime. Jinayah is the masdar (original word) of the verb (fi'il madji) which means work that is intended for humans who have sinned or made mistakes. Jarimah is an act that is prohibited by sharia which is threatened by Allah with had or takzir punishment (15). In this case, as with the word jinayah, the word jarimah also includes doing or not doing, doing or leaving actively or passively (17). Abdul Qadir Audah as quoted by Suharyadi explains this problem by saying that the word prohibition as stated in the definition above means: What is meant by mudharat (prohibition) is doing an act that is forbidden or leaving an ordered act. From this explanation it can be understood that the word mudharat (prohibition) has two meanings (18).

First, prohibition of doing means prohibited from doing forbidden acts. Second, prohibition of not doing or prohibition of keeping silent means leaving (keeping silent) from acts that according to the rules must be done. The expression jarimah is often used as a sinful act, form, type or nature of a major sin. For example, theft, murder, rape or acts related to rebellion. All of these can be called jarimah which are then combined with the unit or nature of the act (19).

In positive law, the terms criminal act, criminal incident, criminal violation, and punishable act are also known, which have the same meaning as crime. All of these are deviations from the Dutch language, strafbaar fait. In the use of the term crime, it is more often used in general legal science, while the term criminal act is often associated with the crime of corruption, which in law is often used as the term criminal act (21). Thus, it can be concluded that the two terms have similarities and differences etymologically. Both terms have one single meaning, have one meaning and have the same meaning and are intended for actions that have negative connotations, are wrong and sinful. The difference lies in the use, direction of the discussion, and in what series the two words are used (22).

The orientation of the prophetic paradigm in enforcing the law is actually "similar" to the idea of progressive law initiated by Satjipto Rahardjo as quoted by Kelik Wardiono where humans and the people are the goal of the law) (23). Progressive law enforcement as quoted by Suparman Marzuki is law enforcement that is subject to the applicable system, but is more affirmative (affirmative law enforcement) (24).

Affirmative means the courage to carry out liberation from conventional practices and affirm the use of other methods, namely breaking through the rules of legal practice that have been going on for a long time. Prophetic Legal Science, it seems necessary to rethink what is actually the material object of prophetic legal science and its differences with Legal Science in general (25). To find out this, what needs to be asked is what is the nature of law itself? In Legal Science in general, there are many basic assumptions adopted by legal scientists to explain what the nature of law itself is (26).

Considering that cybercrime is a crime involving sophisticated devices, positive law is often not implemented properly and therefore cannot protect society (27). Positive law whose sanctions are only imprisonment, fines and detention of course cannot fully handle this non-conventional crime. In this case, the use of a prophetic perspective in law enforcement against cybercrime is an interesting choice with various sanctions ranging from light to heavy. Cyber terrorism perpetrators who claim many victims (such as disrupting air or land traffic lights with

many accident victims) require legal action with a prophetic perspective in an effort to protect society.

CONCLUSION

Given that cybercrime is a crime with sophisticated devices, positive law is often less precise in its application so that it cannot protect society. Cybercrime is a criminal activity that uses computer facilities or computer networks without permission and against the law, either by changing or not changing (damaging) the computer facilities that are entered or used or crimes that use electronic internet media because they are included in the category of cybercrime, or crimes in the computer field against the law. From a prophetic perspective, the punishment for perpetrators of cybercrime varies. From a prophetic perspective, cybercrime (jinayat and jarimah) can be punished with ta'zir. Ta'zir according to the linguistic meaning means prevention (al-man'u). According to the term ta'zir is a punishment that is educational (ta'dib) in the sense of anticipating by intimidating (tankif). In terms of sharia, ta'zir is intended as a sanction imposed on the basis of disobedience with punishments that vary according to the severity of the crime committed. From a prophetic perspective, sanctions are imposed to protect society from cybercrime in order to maintain order and security, not retaliation.

REFERENCES

1. Widodo. Criminal Law Aspects of Mayantara Crimes. Yogyakarta: Aswaja Pressindo; 2013. 5 p.
2. Mansur DMA, Gultom E. Cyberlaw Legal Aspects of Information Technology. Bandung: Refika Aditama; 2009.
3. Widodo. Criminal Law in the Field of Information Technology (Cybercrime Law): Theoretical Review and Campus Analysis. Yogyakarta: Aswaja Pressindo; 2013. 15 p.
4. Hosnah AU, Antoni H, Yofany R. Law Enforcement Against Perpetrators of Defamation Through Social Media Based on the ITE Law. Int J Multicult Multireligious Underst. 2023;10(4):362.
5. Situmeang SMT. Cyber Law. Bandung: Cakra Publisher; 2020. 1 p.
6. Ramli A. Cyber Law and Intellectual Property Rights in the Indonesian Legal System. Bandung: Refika Aditama; 2010. 2–3 p.
7. The Government of the Republic of Indonesia. Law Number 11 of 2008 on Electronic Information and Transactions. Indonesia; 2008.
8. The Government of the Republic of Indonesia. Law Number 36 of 1999 on Telecommunications. Indonesia;
9. Wardiono K. Prophetic: An Epistemological Offer for Legal Studies. J LawJustice. 2019;1(1):17–41. 10.23917/jtl.v1i1.8797

10. Aldriano MA, Priyambodo MA. Cyber Crime from a Criminal Law Perspective. J Citizenship. 2022;6(1). 10.31316/jk.v6i1.2947

11. Maskun. Cybercrime: An Introduction.2014.

12. Wiebe W. Computer-Based Crime. In: Seminar. Makassar; 2000. p. 2.

13. Ash-Shidiqqi EA. Observing Prophetic Legal Science: Godly Law Enforcement. Amnesty J Huk. 2020;2(1):33–42. 10.37729/amnesty.v2i1.701

14. Jannah S, Naufal M. Cyber Crime Law Enforcement Reviewed from Positive Law and Islamic Law. Al-Mawarid. 2012;12(1):81–2.

15. Gunawan H. Cyber Crime in the Perspective of Islamic Jurisprudence. J el-Qanuniy J Sharia Sciences and Social Institutions. 2020;6(1):102–3.

16. Nasution MA. Hoax as a Form of Hudud. J Jurispudentia; J Law Econ Sharia Faculty of Sharia and Legal Sciences IAIN Padangsimpuan. 2017;3(1).

17. Suharyadi, Sampara S, Ahmad K. Cyber Crime in the Perspective of Islamic Law. J Lex Gen. 2020;1(5):762–73. 10.52103/jlg.v1i5.199

18. Al-Qadir AA. At-Tasyri' Al Jinaiy Al –Islamy. Beirut: Dar Al-Kitab Al-Arabi; 2012.

19. Muslich AW. Introduction and Principles of Islamic Criminal Law (Fiqh Jinayah). Jakarta: Sinar Grafika; 2004. 9 p.

20. Syamsudin. Prophetic Law: Initial Ideas, Philosophical Foundations and Possible Developments in the Postmodern Era. Yogyakarta: PSH FH UII; 2013.

21. Chazawi A. Criminal Law Lesson Part 1.2010.

22. Munir A.A.Measuring Prophetic Legal Reasoning in the Political Behavior of Intellectuals (Context of the Constructive Approach of Maqashid Syari'a. Siyastatuna. 2024;4(2).

23. Wardiono K. Prophetic Legal Studies: Description of the Paradigmatic Epistemological Basis [Internet]. Surakarta: Muhammadiyah University Press; 2020.

24. Thontowi J. Prophetic Paradigm in Legal Science Teaching and Research.Unisia [Internet]. 2012;34(76):86–99.

25. Garaudy R, Rasjidi. The Promises of Islam. Jakarta: Bulan Bintang; 1984.

26. Ahimsa-Putra HS. The Prophetic Paradigm: Is It Possible? Is it necessary? In: Prophetic Workshop [Internet]. Yogyakarta: UGM Postgraduate School; 2011.

27. Djanggih H, Qamar N. Application of Criminology Theories in Combating Cyber Crime. Pandecta J Research Law Journal. 2018;13(1):10–23.