At-Tafahum

Vol. 6 No. 2 (2022) pp. 87-90

ISSN : 2580-4707 (online) - 2549-0159 (print)
https://jurnal.uinsu.ac.id/index.php/attafahum/index

Combating Cyber Crime From The Perspective Of Islamic Criminal Law

Aicha Azdina Adly Fesya[1] Rizky Zaidan Ketaren[2]
[1]International Open University Kanifing Gambia
[2]State Islamic University of North Sumatra
E-mail: azdinaaicha19@gmail.com rzaidanketaren@gmail.com

Info Articles

Article History
Received : 2022-09-07
Revised: 2022-09-13
Published: 2022-09-30

Keywords:
Cyber Crime, Islamic Criminal Law, Ta'zir.

Abstract

This article aims to analyze the concept of cybercrime prevention from the perspective of Islamic criminal law and examine its relevance to the development of modern digital crime. The research method used is normative legal research with a conceptual approach and a legislative approach. The data used consists of primary, secondary, and tertiary legal materials analyzed qualitatively. The results of the study indicate that although cybercrime is not explicitly recognized in classical Islamic criminal law literature, the basic principles of jarimah, particularly in the category of ta'zir, can be used to qualify various forms of cybercrime.

I. INTRODUCTION

The development of information and communication technology in the era of globalization has brought significant changes in various aspects of human life. (Barda Nawawi Arief, 2006). The internet as the main medium in digital transformation not only provides easy access to information and communication, but also opens up opportunities for various new forms of crime known as cybercrime. (Maskun, 2013). This crime includes various forms, such as online fraud, hacking, theft of personal data, to the distribution of illegal content that has a broad impact on individuals and society. The characteristics of cybercrime which is borderless, anonymous, and utilizes sophisticated technology makes it difficult to detect and effectively address.

In Indonesia, cybercrime prevention efforts have been implemented through various legal instruments, such as the Electronic Information and Transactions Law (UU ITE) and provisions in the Criminal Code (KUHP). However, the rapid development of crime methods often does not keep pace with the development of existing regulations. This creates a gap between legal norms and the reality of crime in society, necessitating alternative approaches that can provide more comprehensive solutions.

In this context, Islamic criminal law, as part of a legal system that has universal, flexible, and welfare-oriented principles, can be a relevant perspective in tackling cybercrime. Although in the classical literature of Islamic criminal law there is no explicit discussion of cybercrime, the basic principles in the concept of jarimah, especially jarimah ta'zir, provide room for the authorities to determine new forms of crime and their sanctions according to the development of the times and the needs of society (Ahmad Hanafi, 1993). This approach shows that Islamic criminal law has a high adaptability to social and technological dynamics.

Furthermore, Islamic criminal law emphasizes not only repressive aspects through sanctions, but also preventive aspects through moral development, strengthening ethical values, and individual responsibility within society. This holistic approach is crucial in the context of cybercrime, which is not only related to legal violations but also to moral degradation and the misuse of technology.

II. RESEARCH METHODS

This study employs a normative legal research approach, focusing on the study of applicable legal norms, both those contained in legislation and Islamic legal literature. This approach was chosen because the study aims to analyze the concept of cybercrime

Vol. 6 No. 2 (2022) pp. 87-90
ISSN : 2580-4707 (online) - 2549-0159 (print)
https://jurnal.uinsu.ac.id/index.php/attafahum/index

prevention from an Islamic criminal law perspective and examine its relevance to the positive legal system in Indonesia. By using this method, this research is expected to be able to provide an in-depth analysis of how the concept of Islamic criminal law can be used as an alternative approach in dealing with cyber crime, as well as the extent of its relevance in the context of national law in Indonesia.

III. RESULTS AND DISCUSSION

A. Research result

The research results show that cybercrime, as a form of modern crime, has not been specifically regulated in classical Islamic criminal law. However, it can be substantially qualified under the concept of jarimah (delinquency), particularly in the category of ta'zir (delinquency). This is because cybercrime shares elements with several criminal acts in Islamic law, such as fraud (gharar), theft (sariqah), and destruction (ifsad), even though it is committed through digital media. Therefore, determining the type and sanctions for perpetrators of cybercrime can be left to the authorities or ulil amri (rulers of authority) by considering the level of crime and the public interest.

The research results show that cybercrime, as a form of modern crime, has not been specifically regulated in classical Islamic criminal law. However, it can be substantially qualified under the concept of jarimah (delinquency), particularly in the category of ta'zir (delinquency). This is because cybercrime shares elements with several criminal acts in Islamic law, such as fraud (gharar), theft (sariqah), and destruction (ifsad), even though it is committed through digital media. Therefore, determining the type and sanctions for perpetrators of cybercrime can be left to the authorities or ulil amri (rulers of authority) by considering the level of crime and the public interest.

B. Discussion

Cyber crime is a criminal act committed by utilizing information technology facilities, especially the internet and computer networks, to harm other parties through data theft, online fraud, defamation, system destruction, distribution of immoral content, to the distribution of malware and DDoS attacks.

Cybercrime, as a modern crime phenomenon, is a logical consequence of the increasingly rapid development of information technology. This crime has unique characteristics, such as being committed through electronic media, being transnational, and being difficult to trace because perpetrators can conceal their identities anonymously.

From an Islamic criminal law perspective, although cybercrime is not explicitly recognized in classical literature, it can be substantially analogous to several existing forms of crime. For example, online fraud can be linked to the concept of gharar or tadlis (fraud), while hacking and data theft can be analogous to sariqah (theft) in the broad sense. Furthermore, the act of disseminating content that is damaging or detrimental to others can be categorized as a form of ifsad fi al-ardh (destruction on earth) (Abdul Wahhab Khallaf, 1978). Thus, Islamic criminal law has the flexibility to accommodate new forms of crime through the method of ijtihad.

Furthermore, within the framework of Islamic criminal law, cybercrime can generally be classified as a ta'zir crime, a type of crime whose form and sanctions are not explicitly specified in the text, leaving the determination to the authorities or ulil amri (Topo Santoso, 2003). This ta'zir concept provides ample scope for the state to determine punishments appropriate to the severity of the crime, its impact, and the social conditions of the community. This demonstrates that Islamic criminal law is adaptive and responsive to developments, including in addressing technology-based crimes.

Furthermore, combating cybercrime in Islamic criminal law emphasizes not only repressive aspects but also preventive ones. The preventive aspect is realized through the instilling of moral values, ethics, and individual responsibility in the use of information technology. Meanwhile, the repressive aspect is implemented through the application of sanctions aimed at providing a deterrent effect while maintaining order and the public good. This integrative approach between preventive

Vol. 6 No. 2 (2022) pp. 87-90

ISSN : 2580-4707 (online) - 2549-0159 (print)
https://jurnal.uinsu.ac.id/index.php/attafahum/index

and repressive measures is the advantage of Islamic criminal law in comprehensively addressing crime.

Thus, it is understandable that Islamic criminal law has a strong conceptual foundation for combating cybercrime, even though it is not explicitly regulated in classical sources. Through the concept of ta'zir (criminal offenses) and the principle of benefit, Islamic criminal law can provide flexible and contextual solutions to the development of modern crime and can complement Indonesia's national legal system.

1. The concept of Islamic criminal law in dealing with cyber crime

In Islamic criminal law, criminal acts are generally grouped into hudud, qisas/diyyat, and ta'zir.
(asy-Syatibi, 1997).

Cyber crime, because it is not always explicitly stated in the texts (the Qur'an and hadith), tends to be categorized as a ta'zir crime, namely a criminal act for which sanctions are imposed by the authorities or judges to prevent crime and maintain social order.

Ta'zir is flexible and based on the principles of maqasid al-syari'ah, especially the maintenance of five basic human needs (al-maqasid al-khamsah):

1) Hifz Al-Din (Guarding Religion),
2) Hifz Al-Nafs (Guarding The Soul),
3) Hifz Al-Mal (Guarding Wealth),
4) Hifz Al-Nasl (Protecting Descendants/Honor), And
5) Hifz Al-'Aql (Guarding Reason).

Cybercrimes involving fraud, theft of financial data, defamation, the distribution of immoral and pornographic content, and cyber attacks that damage the economic system, clearly violate several of these maqasid, so Islamic criminal law views them as acts that deserve sanctions.

2. Sanctions and redress mechanisms in Islamic criminal law

Punishment for immoral acts that do not receive hudud or qisas punishment, with the aim of preventing and improving morals," which is relevant for cyber crime because it is adaptive to current developments (Wahbah az-Zuhaili, 2011).

In a journal study on cyber crime from an Islamic criminal law perspective, the author generally believes that the main sanction for perpetrators of cyber crime is ta'zir which is imposed through a judicial process by a judge.

Various types of ta'zir punishment in the context of cyber crime can be:

1) Warning/Threat,
2) Prison,
3) Exile,
4) Whipping, Even
5) Death Penalty,
6) Depending On The Level Of Harm (Harm) Caused By The Action.

3. Combating cyber crime: Integration of positive law and Islamic criminal law

Several journals highlight that Indonesian positive law (especially the ITE Law) provides criminal sanctions in the form of imprisonment of up to 10 years and fines of up to 10 billion rupiah, but its enforcement is often hampered by the difficulty of digital evidence, the anonymity of perpetrators, and jurisdictional limitations.

From the perspective of Islamic criminal law, cyber crime is seen as a modern development of previously existing forms of crime (for example fraud, theft, slander, adultery), only carried out using digital technology. In the book Islamic Criminal Law, it is explained that ta'zir includes "all new forms of harm that are not specifically mentioned, including those involving modern tools, with proportional sanctions such as ta'zir badani (flogging) or ta'zir mal (fine). (Abdul Qadir Audah, 2009).

Therefore, many studies offer integrative strategies, namely:

1) filling the gaps in positive law with the principles of Islamic ethics and justice,

Vol. 6 No. 2 (2022) pp. 87-90

ISSN : 2580-4707 (online) - 2549-0159 (print)
https://jurnal.uinsu.ac.id/index.php/attafahum/index

2) strengthening cooperation between law enforcement officers, religious institutions and the community, and
3) develop regulations that are more adaptive to developments in cyber technology.

IV. CONCLUSION AND SUGGESTIONS

A. Conclusion

Based on the discussion above, it can be concluded that cybercrime, as a form of modern crime, is not explicitly recognized in classical Islamic criminal law. However, it can be substantially classified under the concept of jarimah (crime), specifically ta'zir (crime of violation of Islamic law). The flexibility of the ta'zir concept allows authorities to establish legal forms and sanctions appropriate to current developments and the level of crime. Furthermore, Islamic criminal law offers a comprehensive approach through a balance between preventive and repressive measures in combating crime. Thus, Islamic criminal law has strong relevance and can serve as an alternative or complement to the national legal system in addressing the challenges of cybercrime in the digital era.

B. Suggestion

It is necessary to develop more adaptive regulations for cybercrime by integrating Islamic criminal law values, as well as strengthening preventive efforts through moral education and digital literacy in society.

REFERENCE LISTAN

Arief, Barda Nawawi. (2006). Mayantara Crimes: The Development Of Cyber Crime Studies In Indonesia. Jakarta: Rajagrafindo Persada.

Asy-Syatibi. (1997). Al-Muwafaqat Fi Usul Ash-Syari'ah. Volume 2. Dar Al-Kutubi.

Audah, Abdul Qadir. (2009). Islamic Criminal Law. Dar Al-Fikr.

Hanafi, Ahmad. (1993). Principles Of Islamic Criminal Law. Jakarta: Bulan Bintang.

Khallaf, Abdul Wahhab. Ushul Fiqh Science.

Maskun. (2013). Cyber Crime: An Introduction. Jakarta: Kencana.

Topo Santoso. (2003). Grounding Islamic Criminal Law: Enforcing Sharia In Discourse And Agenda. Jakarta: Gema Insani Press.

Zuhaili, Wahbah. (2011). Fiqh Jinayat. Indonesian Translation. Azzam Library.

.