Case Studies of Contemporary Crimes from an Islamic Law Perspective

Muhammad Farrel Aufa Nst[1] Nanda Syahputra[2]
[12]State Islamic University Of North Sumatera
E-mail: muhammadfarrrelaufanasution@gmail.com syahputraananda1012@gmail.com

Info Articles

Article History
Received: 2024-09-07
Revised: 2024-09-14
Published: 2024-09-30

Keywords:
Contemporary Crime, Cybercrime, Positive Law, Jinayah Fiqh.

Abstract

The acceleration of modern-day information technology acts as a double-edged sword, triggering a radical metamorphosis of conventional crime into contemporary cyber-based crime. This study aims to analyze the characteristics, typology, and causal factors of contemporary crime, as well as formulate the qualifications of crimes and the formulation of sanctions from the perspective of Indonesian positive law and Islamic Criminal Law (Fiqh Jinayah). The research method used is normative juridical with a conceptual approach and case studies of four crime typologies, namely online fraud, cyber-corruption, ransomware attacks, and the industrialization of hoaxes. The results show that contemporary crimes are characterized by de-territoriality, high anonymity, fluidity, and are included in the white-collar crime cluster triggered by the technological gap and the degradation of cyber ethics. Although Indonesian positive law has anticipated this crime through the instruments of the ITE Law, the Corruption Law, the Money Laundering Law, and Law No. 1 of 1946, the effectiveness of its enforcement is still hampered by the complexity of digital evidence and jurisdictional constraints. In the view of Islamic Jurisprudence, all of these contemporary crimes cannot be categorized as hudud or qisas-diyat because they do not fulfill rigid material requirements of sharia, such as the absence of physical storage restrictions (al-hirz) on data theft. Therefore, contemporary crimes are classified as Ta'zir crimes, where the authority to formulate sanctions and their formulation is completely handed over to the ijtihad of the ruler (ulil amri) in order to uphold the public interest (mashlahah mursalah) and fortify the pillars of al-maqasid al-khamsah.

I. INTRODUCTION

The acceleration of information technology in the modern era acts as a double-edged sword, triggering a radical metamorphosis of conventional crime into contemporary cybercrime. These crimes are highly fluid, transcend territorial boundaries, possess a high degree of anonymity, and fall into the white-collar crime cluster. The concrete manifestation of this phenomenon is reflected in the massive proliferation of four crime typologies in society: online fraud, cyber-based corruption, ransomware attacks, and the industrialization of hoaxes. The massive development of this digital modus operandi often triggers obstacles to law enforcement due to the complexity of digital evidence and jurisdictional constraints in Indonesian positive legal instruments such as the ITE Law, the Corruption Law, and the Money Laundering Law. (Ramadan, 2022).

This dynamic also demands a fundamental juridical-theological response from the Islamic Criminal Law system (Fiqh Jinayah). As a universal legal system, Islam is required to address the legal status of every new criminal act. However, classical legal texts often face textual problems when dealing with digital methods. For example, in the crime of digital asset theft via cyberspace, the material requirements for the punishment of amputation, such as the requirement for a physical safe storage location (al-hirz), are no longer met. The gap between the development of cyber modus operandi and the rigidity of legal texts in both positive law and classical fiqh is the primary urgency of this research.(Mubarok, 2018).

To examine these issues, this research applies a normative juridical method with a conceptual and case study approach. Primary legal materials, in the form of domestic legislation, are juxtaposed

with secondary legal materials sourced from classical Islamic criminal law books across schools of thought and accredited legal journals. All collected literature data is then analyzed qualitatively and descriptively using deductive reasoning methods to produce systematic and comprehensive conclusions.(Santoso, 2020).

This study aims to analyze the characteristics, typology, and causal factors of cybercrime, as well as reconstruct the qualifications of the offense and the formulation of its sanctions. From the perspective of Islamic criminal law, this group of contemporary crimes is classified as Jarimah Ta'zir because it does not meet the rigid requirements for proof of hudud or qisas. Therefore, the authority to formulate sanctions is entirely handed over to the ijtihad of the ruler (ulil amri) based on the principle of public benefit in order to fortify the pillars of the objectives of Islamic law (al-maqasid al-khamsah), especially in protecting life, mind, and property in cyberspace.(Muslich, 2021).

II. RESEARCH METHODS

This study uses a normative legal research method (doctrinal legal research) through a library research approach with an analytical focus on norms, principles, doctrines, and legal regulations related to contemporary cybercrime. The applied approach includes a conceptual approach to dissect the nature of the offense and a case study approach to four main typologies of cybercrime. Data were collected from primary legal materials in the form of laws and regulations (Law No. 1 of 1946, the ITE Law, the Corruption Law, and the Money Laundering Law) as well as secondary legal materials such as classical Fiqh Jinayah books, cyber literature books, and reputable scientific journals. All legal materials were then analyzed qualitatively and descriptively using a deductive reasoning method to systematically reconstruct the qualifications of cybercrime into the Jarimah Ta'zir group.

III. RESULTS AND DISCUSSION

A. Typology, Characteristics, and Causality Factors of Contemporary Cybercrime

The evolution of information technology has given rise to a new criminal landscape that is fundamentally different from conventional crimes. Within the dynamics of modern law, there are four typologies of contemporary cyber-based crimes that have massive destructive power in society: online fraud, cyber-corruption, ransomware attacks, and the industrialization of hoaxes.(Ramadan, 2022)These four crimes are characterized by highly fluid characteristics, a high degree of anonymity through digital identity manipulation, and a nature that transcends state jurisdiction (de-territorial).(Hamdan, 2020)As a result, the boundaries of traditional criminal law based on physical territorial sovereignty have become blurred and complicate the process of enforcing national criminal law.(Raharjo, 2021).

From a criminological perspective, the spread of contemporary cybercrime is triggered by two main causal factors, namely external factors in the form of technological security gaps and internal factors in the form of degradation of cyber ethics.(Mansur, 2019)The speed of software innovation is often not matched by adequate data protection systems, creating vulnerabilities that criminals exploit. However, these technical vulnerabilities will not result in criminal offenses without malicious intent (mens rea) arising from the decline in moral values and legal compliance in cyberspace. The phenomenon of online fraud and the industrialization of hoaxes, for example, reflects how digital space is used as an instrument of social manipulation for short-term economic gain at the expense of the constitutional rights of other citizens.

B. Legal Obstacles to Digital Evidence in Indonesian Positive Legal Instruments

The Indonesian government has actually anticipated the development of this cybercrime by establishing layers of

regulations, ranging from general provisions in Law No. 1 of 1946 (the Old Criminal Code) to specific regulations (lex specialis) such as the ITE Law, the Corruption Law, and the Money Laundering Law. However, in the realm of practical criminal law enforcement, these regulations often hit a thick wall, leading to legal uncertainty. The most crucial legal obstacle lies in the aspect of proving digital evidence (Raharjo, 2021). Unlike conventional evidence in the form of inanimate objects or physical documents, digital evidence is extremely fragile, easily manipulated, altered, and even deleted in a matter of seconds without leaving any visible physical traces.

The process of standardizing the handling of digital evidence (digital chain of custody) in Indonesia still faces serious obstacles, both in terms of the capacity of law enforcement officers and the availability of digital forensic laboratories. The validity of electronic evidence in court is often debated due to the potential for data contamination during the seizure process. Furthermore, the transnational nature of cybercrime demands mutual legal assistance between countries. When data servers or cybercriminals are located outside of Indonesia's legal jurisdiction, the investigation process often reaches a dead end due to jurisdictional conflicts and complex international bureaucracy, making it difficult to realize the principles of a fast, simple, and low-cost justice system.

C. Reconstruction of Cybercrime into the Ta'zir Crime Group

When this issue of cyber law is drawn into the discourse of Islamic Criminal Law (Fiqh Jinayah), Islamic legal scholars are faced with a textual challenge to classical fiqh texts. In classical fiqh, criminal acts punishable by definitive punishment (hudud) have very strict and rigid material requirements.(Audah, 2019)For example, in the crime of theft (sarisah), the perpetrator can be sentenced to have his hand amputated if he fulfills the condition of having taken goods from a safe and locked storage place (al-hirz).(Sabiq, 2018)In cases of data breaches or digital asset theft via cyberattacks, physical storage space no longer exists because it has been transferred to a cloud storage system or virtual database.

Due to the failure to fulfill the material elements of al-hirz physically and the existence of syubhat (ambiguity) regarding the nature of absolute ownership of digital commodities, contemporary cybercrime cannot be classified into the categories of Jarimah Hudud or Qishash-Diyat.(Mubarok, 2018)To avoid a legal vacuum (rechtvacuum), Islamic Criminal Law reconstructs the law by incorporating all typologies of cybercrime into the category of Ta'zir crimes. The conceptualization of Ta'zir crimes provides legal flexibility for the Islamic legal system, where the qualifications of crimes and the formulation of sanctions are not textually stipulated in the Qur'an and Hadith, but are left entirely to the ijtihad and legislative authority of the rulers (ulil amri).(Muslich, 2021).

D. Formulation of Ta'zir Sanctions Based on the Principles of Maslahah Mursalah and Maqasid al-Shari'ah

Delegating the authority to formulate Ta'zir sanctions to those in power (ulil amri) does not allow for arbitrary action. The formulation of sanctions against cybercriminals must be based on the principle of public welfare (mashlahah mursalah) to achieve a harmonious social order (Syamnur & Sinaga, 2024). Those in power have the authority to formulate contemporary sanctions relevant to the perpetrator's modus operandi, such as high financial fines, permanent blocking of digital access, and even imprisonment commensurate with the level of economic or social damage caused by the offense (Muslich, 2021). This criminalization policy aligns with the principles of modern law enforcement, which prioritizes deterrence and protection for the wider community.

Philosophically and theologically, the formulation of Ta'zir sanctions against

contemporary cybercrime is a concrete manifestation of efforts to maintain the five main pillars of Islamic law (al-maqasid al-khamsah) in the digital era (Syamnur & Sinaga, 2024). Firm action against online fraud and ransomware is a form of protection for property (hifz al-mal). Eradicating the industrialization of hoaxes and cyber corruption is essential to maintaining the stability of public common sense (hifz al-'aql) and protecting the safety of people's lives (hifz an-nafs) from social conflict triggered by massive misinformation. Thus, the integration of responsive positive legal regulations with the principle of maslahah in Islamic Jurisprudence will produce a formulation of cyber law that not only has legal certainty but also substantive justice (Syamnur & Sinaga, 2024).

IV. CONCLUSION AND SUGGESTIONS

A. Conclusion

Contemporary cybercrime (online fraud, cyber corruption, ransomware, and the industrialization of hoaxes) is characterized by de-territoriality, high anonymity, and falls into the white-collar crime cluster, stemming from technological gaps and the degradation of cyber morality. In Indonesia, although positive legal instruments such as the ITE Law, the Corruption Law, and the Money Laundering Law have been established, their effective enforcement still faces crucial legal obstacles, particularly in terms of the standardization of digital evidence that is vulnerable to manipulation and the limitations of international jurisdiction. From the perspective of Islamic Criminal Law (Fiqh Jinayah), all typologies of contemporary cybercrime are reconstructed into the group of Jarimah Ta'zir (Ta'zir) crimes due to the failure to fulfill rigid material requirements for hudud proof, such as the absence of physical storage space (al-hirz) restrictions in data theft crimes. Therefore, the formulation of sanctions is left to the ijtihad of the rulers (ulil amri) based on the principle of public welfare (mashlahah mursalah) in order to fortify the pillars of al-maqasid al-khamsah, especially in preserving the souls, minds, and property of the people in the digital space.

B. Suggestion

Progressive reform of national criminal procedure law policy is needed through standardization of digital evidence handling (digital chain of custody), increasing the digital forensic capacity of officers, and strengthening cross-border mutual legal assistance agreements to overcome jurisdictional barriers.

LIST OF REFERENCES

Audah, Abdul Qadir. (2019). *Al-Tasyri' al-Jina'i al-Islami Muqaranan bi al-Qanun al-Wadl'i*. Volume 2. Beirut: Dar al-Katib al-Arabi.

Hamdan, M. (2020). "Karakteristik Tindak Pidana Siber dalam Perspektif Kriminologi." *Jurnal Hukum dan Peradilan*, Vol. 9, No. 1, hlm. 34–50.

Kementerian Agama RI. (2019). *Al-Qur'an dan Terjemahannya*. Jakarta: Lajnah Pentashihan Mushaf Al-Qur'an.

Mansur, Didik M. (2019). *Cyberlaw: Hukum Pidana di Ruang Siber*. Bandung: Refika Aditama.

Mubarok, Jaih. (2018). "Kontekstualisasi Hukum Pidana Islam dalam Menghadapi Cybercrime." *Jurnal Hukum Islam Al-Jinayah*, Vol. 4, No. 2, hlm. 152–160.

Muslich, Ahmad Wardi. (2021). *Hukum Pidana Islam (Fiqh Jinayah)*. Jakarta: Amzah.

Raharjo, Agus. (2021). "Cybercrime: Pemetaan Modus dan Problem Penegakan Hukumnya di Indonesia." *Jurnal Hukum Mimbar Justitia*, Vol. 12, No. 2, hlm. 210–238.

Ramadhan, Chazali H. (2022). *Sosiologi Kriminalitas Digital dan Kebijakan Hukum Pidana Indonesia*. Jakarta: Sinar Grafika.

Sabiq, Sayyid. (2018). *Fiqh us-Sunnah*. Volume 3. Kairo: Darul Fath.

Santoso, Topo. (2020). *Menggagas Hukum Pidana*

Islam di Indonesia: Teori dan Praktik. Depok: Rajawali Pers