Ann PUBLISHER
Journal of Law Sciences (Legisci)
e-ISSN 3030-9549
p-ISSN 3032-7555

The Model Of Islamic Criminal Law Enforcement Against Cyber Crime: (An Integrative Analysis of the Maqāṣid al-Sharī'ah Approach and Modern Cyber Law in Addressing the Challenges of Transnational Digital Crimes)

Achmad Kholiq[1], **Akhmad Shodikin**[2], **Faishal Rahim**[3]
[1]UIN Cyber Syekh Nurjati Cirebon, Indonesia, Email achmadkholiq672@gmail.com
[2]UIN Cyber Syekh Nurjati Cirebon, Indonesia, Email shodikin73@uinssc.ac.id
[3]University of Kuningan, Indonesia, Email faishalrahimi@uniku.ac.id
Corresponding Author: Email achmadkholiq672@gmail.com

Abstract:
Background. The advancement of digital technology has given rise to new forms of crimes known as cyber crimes, characterized by their transnational nature, rapid execution, and difficulty in being confined by state jurisdiction. Modern positive law has responded to this challenge through the formulation of cyber law, regulated at both national and international levels. In contrast, Islamic criminal law provides a normative framework derived from the concepts of jarīmah, ḥudūd, qiṣāṣ, and ta'zīr.
Aims. This article aims to analyze the model of Islamic criminal law enforcement against cybercrime and compare it with modern cyber law.
Methods. The research employs a normative-comparative methodology, incorporating both conceptual and regulatory analysis.
Result. The findings reveal that Islamic criminal law offers universal principles applicable to cybercrime through the category of ta'zīr, which grants discretionary authority to the judge (qāḍī) in determining punishments based on public interest (maṣlaḥah). Meanwhile, modern cyber law emphasizes procedural aspects, digital evidence, and international mechanisms of enforcement. The comparative analysis indicates a convergence between the two systems in their objectives of protecting society, though they differ in terms of legitimacy sources and normative foundations.
Conclusion. Hence, an integrative model of enforcement that combines the maqāṣid al-sharī'ah with modern cyber law instruments could serve as a strategic alternative in addressing the complexity of cybercrime.
Implication. Cybercrime law enforcement cannot rely on a single legal system. Instead, an integrative framework is needed to unite the strengths of Islamic criminal law and modern cyber law, thereby producing a more comprehensive, practical, and just cyber legal order in addressing the challenges of the digital age.

Keywords: Islamic criminal law, cyber crime, cyber law, *maqāṣid al-sharī'ah*, *fiqh jināyah*

INTRODUCTION

The development of information and communication technology has brought fundamental changes to the patterns of social, economic, political, and legal interactions in the digital era. On the one hand, this transformation provides convenience, efficiency, and accelerated access to various aspects of life; on the other hand, it has also generated new problems in the form of cyber crimes. These crimes emerge as a logical consequence of digital globalization, which eliminates spatial and temporal boundaries, allowing perpetrators to operate across borders with minimal risk yet producing significant impact. Unlike conventional crimes, cyber crimes are transnational, technologically sophisticated, difficult to detect, and often involve complex digital systems (Wall, 2020).

In the context of modern law, cybercrime is generally understood as unlawful conduct involving the use of computers, the internet, or digital devices as either the means or the objects of criminal acts. In Indonesia, Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), along with its amendments, provides the juridical framework for regulating and enforcing laws against cyber crimes. These include data theft, online fraud, illegal content dissemination, system hacking, and digital copyright infringement (Nasution, 2020). At the international level, the *Budapest Convention on Cybercrime* (2001) serves as a widely recognized global legal instrument, classifying cyber crimes into major categories, ranging from attacks on the confidentiality and integrity of computer systems to content-related crimes and intellectual property violations (Clough, 2015).

Nevertheless, the perspective of Islamic law must also be considered in addressing this phenomenon. Although neither the Qur'an nor Hadith explicitly mentions cyber crime, *fiqh jināyah* as the Islamic criminal law system provides a flexible framework for understanding contemporary offenses. Principles of analogy (*qiyās*) and *siyāsah shar'iyyah* enable Muslim jurists (*fuqahā'*) and Islamic legal authorities to classify cyber crimes into specific *jarīmah*. For instance, data theft and online account hacking can be analogized with *jarīmah sariqah* (theft), digital defamation with *jarīmah qadhf* (false accusation), and the distribution of pornography with *jarīmah fāḥishah* (immoral acts) (Auda, 2008).

The significance of a comparative study between modern positive law and Islamic criminal law lies in the pursuit of a more holistic enforcement model. While modern law provides systematic, formal, and internationally applicable legal instruments, Islamic law contributes ethical, moral, and transcendental dimensions that emphasize justice and the preservation of public welfare. The integration of both approaches becomes increasingly

relevant since cybercrime is not only a legal issue but also a moral and social responsibility. Therefore, an integrative analysis between Islamic criminal law and modern cyber law is crucial in developing a framework of enforcement that is just, humane, and aligned with the objectives of *maqāṣid al-sharī'ah*.

This study gains further importance when considering the wide-ranging impact of cyber crimes, which threaten the five essential objectives of *maqāṣid al-sharī'ah*: protection of religion (*ḥifẓ al-dīn*), life (*ḥifẓ al-nafs*), intellect (*ḥifẓ al-'aql*), lineage (*ḥifẓ al-nasl*), and property (*ḥifẓ al-māl*). Online fraud undermines property protection; hate speech disrupts the safeguarding of intellect and dignity; while the spread of digital pornography threatens lineage protection and public morality. Hence, countering cybercrime cannot solely rely on modern legal instruments, but must also be reinforced by the ethical and spiritual principles of Islamic law, which emphasize the prevention of harm (*daf' al-mafāsid*) and the promotion of public interest (*jalb al-maṣāliḥ*) (Hallaq, 2009).

Given these complexities, this research on The Model of Islamic Criminal Law Enforcement Against Cyber Crime: An Integrative Analysis with Modern Cyber Law serves as an effort to identify both the conceptual and practical points of convergence between the two legal systems. The comparative approach is expected to contribute theoretically to the development of legal studies while providing practical guidance for law enforcement agencies and religious institutions in confronting the challenges of cybercrime in the modern era.

LITERATURE REVIEW

Both international and national legal scholars have extensively discussed studies on cybercrime and cyber law. David S. Wall (2007) emphasized that the development of digital technology has transformed traditional crimes into more complex, transnational, and difficult-to-detect cybercrimes. This view is consistent with Jonathan Clough (2010), who highlighted the fundamental challenges of criminal law in addressing cybercrime, particularly issues of evidence, jurisdiction, and offender identification, which remain the most significant obstacles in the implementation of positive law. Susan W. Brenner (2010) further argued that cybercrime is not merely a legal issue but also encompasses social and global security dimensions, necessitating a new legal framework.

In the Indonesian context, Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) and its amendment through Law No. 19 of 2016 serve as key

instruments in cyber law enforcement. Several studies on positive law have pointed out the weaknesses of the ITE Law, particularly in relation to privacy protection, over-criminalization, and limited international coordination (Sutedi, 2012; Sembiring, 2018). These studies indicate that despite the progress in modern regulations, legal loopholes still exist and are frequently exploited by digital offenders.

Meanwhile, in the tradition of Islamic law, explicit discussions of cybercrime are absent in classical literature. However, the principles of Islamic criminal law (fiqh jināyah) outlined by Wahbah al-Zuḥailī (1989) in *al-Fiqh al-Islāmī wa Adillatuh* provide a broad basis for applying the concept of *jarīmah*, particularly within the category of *ta'zīr*, to address contemporary crimes unfamiliar to classical jurists. Mohammad Hashim Kamali (2003) emphasized the importance of *maqāṣid al-sharī'ah* as a dynamic normative framework in dealing with social change, including the rise of modern technologies. These perspectives suggest that Islamic criminal law has the adaptability to respond to cybercrime while upholding the principles of justice, protection of rights, and public interest.

Several contemporary studies have attempted to bridge Islamic law with digital crime. For instance, Al-Dawoody (2011) explored Islamic humanitarian law and demonstrated how sharī'ah principles can be contextualized within modern international regulations. Similarly, Abou El Fadl (2014) highlighted the flexibility of sharī'ah in responding to new phenomena through collective *ijtihād*. In the Indonesian context, Hidayat (2019) examined the application of the *ta'zīr* concept in addressing cybercrime, although there remains a scarcity of studies that systematically compare Islamic criminal law with modern cyber law.

From this literature review, three major trends in previous research can be identified: first, studies on cybercrime and the challenges of positive law; second, analyses of classical *fiqh jināyah* and the relevance of *maqāṣid al-sharī'ah* to contemporary issues; and third, attempts at integrating Islamic law with modern legal frameworks. However, specific studies that examine models of Islamic criminal law enforcement against cybercrime in comparison with modern cyber law are still very limited. Therefore, this study offers an original contribution by proposing an integrative approach that has not been widely explored in previous scholarship.

METHOD

This study employs normative legal research with a qualitative approach. Normative legal research is appropriate since the primary focus is the analysis of legal texts, both derived from Islamic law and modern positive law, in order to identify relevant principles, concepts, and enforcement models concerning cybercrime. The normative approach is used to explore and analyze legal norms contained in *fiqh jināyah*, *maqāṣid al-sharī'ah*, as well as positive regulations such as national and international cyber law.

The methodological framework consists of several approaches. First, a **conceptual approach**, which examines the fundamental concepts of Islamic criminal law (*jarīmah, ḥudūd, qiṣāṣ,* and *ta'zīr*) and modern cyber law. Second, a **comparative approach**, which compares the principles and practices of Islamic criminal law enforcement with modern cyber law instruments, both in terms of substantive norms and enforcement mechanisms. Third, a **historical approach**, which traces the evolution of Islamic law and positive law in addressing contemporary crimes.

The data sources for this research consist of primary and secondary legal materials. Primary sources include the Qur'an, Hadith, classical and contemporary *fiqh* texts, as well as positive regulations such as Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) and its amendments, and international instruments such as the Budapest Convention on Cybercrime. Secondary sources include academic literature, research findings, international journal articles, and works of Islamic legal scholars and cyber law experts.

The data analysis technique employed is content analysis, which involves the following steps: (1) identifying the concepts and legal norms of Islamic criminal law relevant to cybercrime; (2) examining modern cyber law regulations; (3) comparing the principles, objectives, and enforcement mechanisms of both legal systems; and (4) formulating an integrative model of Islamic criminal law enforcement against cybercrime that is applicable to global challenges.

Through this methodology, the study seeks to produce a comprehensive and systematic analysis, thereby contributing to the development of Islamic criminal law theory while simultaneously enriching contemporary cyber law literature.

DISCUSSION

The Concept of Cybercrime in Positive Law and Islamic Law

In positive law, cybercrime is defined as a criminal act committed through the use of information technology, particularly computers and the internet, whether as instruments or as objects of crime. Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) and its amendments provide a legal framework for various types of cybercrime, including data theft, dissemination of illegal content, online fraud, hacking, and crimes against electronic systems. At the international level, the *Budapest Convention on Cybercrime* (2001) expands this scope by classifying cybercrime into four main categories: crimes against the confidentiality, integrity, and availability of computer systems; content-related offenses; computer-related offenses such as fraud and forgery; and copyright violations in the digital domain (Clough, 2015).

From the perspective of *fiqh jināyah* (Islamic criminal jurisprudence), although cybercrime is not explicitly mentioned in classical texts, it can be understood as a form of contemporary *jarīmah* (crime) that resembles classical offenses. For instance, hacking and data theft may be analogized with *jarīmah sariqah* (theft), the spread of false information with *jarīmah qadhf* (false accusation/defamation), and the distribution of pornographic material with *jarīmah fāḥishah* (indecent acts) (Auda, 2008). Hence, *fiqh jināyah* demonstrates flexibility in addressing new forms of crime through the principles of *qiyās* (analogical reasoning) and *siyāsah shar'iyyah* (policy-based governance).

The common ground between positive law and Islamic law in defining cybercrime lies in their acknowledgment of the harm it poses to individuals and society. Both legal systems emphasize the protection of fundamental rights, such as property rights, dignity, and information security. However, a key difference lies in their sources of legitimacy: positive law is grounded in legislation and international conventions, while Islamic law is rooted in the Qur'an, Hadith, and *uṣūl al-fiqh* principles interpreted by jurists.

Principles of Responsibility and *Maqāṣid al-Sharī'ah* in Addressing Cybercrime

The principle of responsibility in Islamic law is fundamentally individual, as every person is accountable for their actions before God and in worldly courts. Nevertheless, responsibility can also become collective when violations have widespread impacts on social stability. In the context of cybercrime, perpetrators bear personal accountability, while the state, as *walī al-amr* (legitimate authority), holds a collective obligation to prevent broader harm (*mafsadah*), as unchecked harm threatens public order and digital security (Kamali, 2019).

The classification of *jarīmah* in Islamic law allows cybercrimes to be categorized primarily under *jarīmah ta'zīr*, since no explicit textual provisions address them. *Jarīmah ta'zīr* is inherently flexible, enabling the imposition of sanctions proportionate to the needs of the time. However, in certain cases, cybercrimes may overlap with *jarīmah ḥudūd*, such as illegal access to digital accounts resembling *sariqah* (theft). If the conditions of *sariqah* are fulfilled, the case could potentially be examined under the *ḥudūd* framework, although in practice it is often adjudicated through *ta'zīr*. Furthermore, *siyāsah shar'iyyah* grants the government authority to introduce new penal policies aimed at safeguarding public interest (*maṣlaḥah mursalah*), thereby legitimizing modern regulations such as cyber laws and data security measures (Hallaq, 2009).

In practice, the role of the *qāḍī* (Islamic judge) is vital in filling legal gaps left by textual sources. Since the classical period, judges have been entrusted with *ijtihād* (independent reasoning) when dealing with cases not explicitly regulated. This role remains highly relevant in the modern era, where judges must employ *qiyās* and incorporate the principles of *maqāṣid al-sharī'ah* to adjudicate cybercrime cases. Such an approach ensures rulings are not merely legalistic but also infused with ethical and spiritual considerations.

Moreover, *maqāṣid al-sharī'ah* has direct relevance in combating cybercrime. The five essential objectives of Sharī'ah—protection of religion (*ḥifẓ al-dīn*), life (*ḥifẓ al-nafs*), intellect (*ḥifẓ al-'aql*), lineage (*ḥifẓ al-nasl*), and property (*ḥifẓ al-māl*)—are all threatened by digital crimes. For example, online fraud undermines property rights, the spread of pornography damages lineage and public morality, while hate speech or disinformation on social media may harm intellect, dignity, and social cohesion. Hence, the enforcement of Islamic criminal law against cybercrime aims not only at maintaining social order but also at achieving universal welfare in line with the objectives of *maqāṣid al-sharī'ah* (Auda, 2010).

This orientation distinguishes Islamic law from modern positive law, as the former does not merely emphasize legalistic dimensions but also moral, spiritual, and transcendental aspects. Cyber law enforcement in the Islamic perspective is not solely repressive but also preventive and educative, instilling awareness that violations in cyberspace are as serious as those in the physical world. Through this approach, the integration of Islamic law and modern positive law in addressing cybercrime may produce a more comprehensive, just, and welfare-oriented enforcement model.

Models of Modern Cyber Law Enforcement

The enforcement of cyber law in modern contexts rests on strong foundations through both international and national legal instruments. One of the most significant milestones is the *Budapest Convention on Cybercrime* (2001), the first international treaty comprehensively regulating cyber offenses, investigative procedures, and cross-border cooperation. The convention categorizes cybercrime into several types, including attacks on the confidentiality and integrity of computer systems, computer-related crimes, content-related offenses, and digital copyright infringements (Clough, 2015). In addition, the United Nations (UN), through its *Guidelines on Cybercrime*, emphasizes the importance of harmonizing legal frameworks among states and safeguarding human rights during law enforcement processes (UNODC, 2019).

At the national level, various countries have enacted specific regulations to address cybercrime. In Indonesia, the primary legal basis is the ITE Law (Law No. 11 of 2008) and its amendment by Law No. 19 of 2016. This regulation covers illegal access, unauthorized interception, data manipulation, dissemination of illicit content, and online defamation. It also authorizes law enforcement agencies to conduct investigations and prosecutions based on digital evidence (Nasution, 2020).

A key principle in modern cyber law enforcement is the *due process of law*, ensuring that every enforcement step adheres to fair legal procedures. This principle is closely tied to the protection of individual privacy rights as part of fundamental human rights. Furthermore, modern regulations emphasize digital consumer protection, particularly in electronic transactions and data privacy. This has become increasingly urgent with the rapid expansion of e-commerce and cross-border digital services (Kuner, 2020).

Nevertheless, cyber law enforcement faces major challenges. First, the transnational nature of cybercrime, where attacks can occur across jurisdictions while positive law remains territorially bound. Second, the fragile nature of digital evidence, which can be easily manipulated, deleted, or concealed, necessitating advanced digital forensic mechanisms. Third, the rapid pace of technological development often outstrips the adaptability of legal regulations, resulting in a gap between emerging cybercrime forms and available legal instruments—a phenomenon commonly referred to as the "legal gap" in modern legal systems (Brenner, 2010).

Thus, although modern cyber law has established a more transparent and more systematic legal framework compared to earlier periods, the challenges of globalization,

technological innovation, and the protection of fundamental human rights remain central issues that demand continuous regulatory innovation and international cooperation.

Comparative Analysis: Islamic Criminal Law vs. Modern Cyber Law

A comparative analysis between Islamic criminal law and modern cyber law demonstrates that although both emerged from distinct historical, epistemological, and sociological contexts, they share a common objective: to establish legal justice, maintain social order, and protect society from the destructive impact of crime. Islamic criminal law positions *maqāṣid al-sharīʿah* as its normative foundation, explicitly aiming to preserve religion, life, intellect, lineage, and property. This principle closely corresponds with the objectives of modern positive law, which seeks to safeguard human rights, public security, and collective interests in the digital society. Hence, the first point of convergence lies in their orientation toward protection and prevention. Both Islamic law and modern positive law affirm that crime prevention is as vital as punishment, since the primary function of law is to ensure societal continuity and prevent harm (*darʾ al-mafāsid*) (Auda, 2008).

Another similarity lies in their shared commitment to legal justice. Islamic criminal law emphasizes the universal principle of *al-ʿadl*, while modern positive law underscores *due process of law* as the cornerstone of justice. In the context of cybercrime, both systems seek to guarantee victim protection, impose proportionate sanctions on offenders, and shield society from further harm. Practically, Islamic criminal law employs *fiqh jināyah* to classify crimes into categories of *ḥudūd*, *qiṣāṣ*, and *taʿzīr*, whereas modern positive law categorizes cybercrime through formal regulations such as the Budapest Convention on Cybercrime and Indonesia's ITE Law. Although the terminology differs, the essence of both legal systems converges on achieving balanced social justice between individual rights and collective interests (Kamali, 2019).

Nevertheless, fundamental differences are also evident. Islamic criminal law is rooted in the legitimacy of divine revelation—*al-Qurʾān* and *ḥadīth*—as its primary sources, interpreted through juristic reasoning (*ijtihād*) within the framework of *uṣūl al-fiqh*. Conversely, modern cyber law derives legitimacy from state consensus, expressed through national legislation and international conventions. This divergence in sources of legitimacy has implications for the nature of sanctions. In Islamic law, *ḥudūd* penalties are fixed, being determined directly by the scriptural texts, while *taʿzīr* punishments are flexible and left to judicial or political discretion. By contrast, cyber law sanctions are established through

temporal legislative processes and can evolve in line with social and technological developments. Thus, Islamic criminal law embodies a transcendental legitimacy, while modern positive law emphasizes procedural legitimacy and political consensus (Hallaq, 2009).

Another distinction lies in regulatory flexibility. While Islamic criminal law prescribes fixed sanctions for *jarāʾim ḥudūd*, it also accommodates adaptability through *taʿzīr* and *siyāsah sharʿiyyah*, enabling responses to novel crimes not explicitly addressed in the classical texts. This flexibility constitutes a distinctive strength of Islamic law: the coexistence of moral-transcendental values with adaptive mechanisms for contemporary phenomena such as cybercrime. For instance, hacking can be analogized to *jarīmah sariqah* (theft), while spreading false information may be likened to *jarīmah qaḏf* (false accusation). Guided by *maqāṣid al-sharīʿah*, Islamic criminal law maintains its relevance in addressing ever-evolving digital realities (Auda, 2010).

In contrast, modern cyber law excels in procedural and technical detail. Its legal frameworks provide systematic mechanisms for investigation, prosecution, and adjudication, all bound by the principle of *due process of law*. Moreover, modern law includes technical instruments such as digital forensics and international cooperation mechanisms, which are essential for tackling transnational cybercrime. For example, the Budapest Convention not only defines cyber offenses but also establishes rules for evidence preservation and cross-border exchange—elements absent in classical Islamic law. This underscores the advantage of modern cyber law in addressing the technical-procedural demands of the digital era (Brenner, 2010).

From an integrative perspective, there is significant potential to combine the ethical-normative dimensions of Islamic criminal law with the formal-legal frameworks of modern cyber law. Such integration could yield a model of law enforcement that balances legality and procedure with moral and transcendental values. For instance, data protection in modern law can be reinforced by the Islamic concept of *amānah* (trust), framing privacy violations not only as legal offenses but also as moral betrayals. Similarly, *taʿzīr* penalties could be adapted to address emerging cybercrimes, while modern instruments such as digital forensics enhance evidentiary effectiveness. Integration would thus produce a more comprehensive enforcement model—procedurally just, normatively adaptive, and morally grounded (Kuner, 2020).

This analysis suggests that the dialogue between Islamic criminal law and modern cyber law should not be framed as a dichotomy but rather as an opportunity for mutual enrichment. In an increasingly complex digital environment, Islamic law contributes an ethical foundation and *maqāṣid*-based orientation toward public welfare, while modern law offers procedural instruments and international cooperation mechanisms suited to the global nature of cybercrime. Their synthesis holds the potential for a hybrid legal model capable of addressing digital challenges without losing the spiritual and moral dimensions characteristic of Islamic law.

From a philosophical standpoint, Islamic law is rooted in a normative-transcendental paradigm, emphasizing human accountability before God as the ultimate source of truth. Thus, legal violations are not only social but also moral-spiritual infractions, affecting one's vertical relationship with God. This contrasts with modern cyber law, which is grounded in legal positivism, treating law as a socially and politically valid consensus without transcendental dimensions. Consequently, Islamic law prioritizes *taḥdhīb al-nafs* (soul purification) through educative sanctions, while modern law emphasizes deterrence and social engineering through formal penal threats (Esposito & DeLong-Bas, 2018).

In practice, Islamic law's *taʿzīr* category provides greater judicial flexibility, enabling sanctions tailored to contemporary conditions and offender characteristics. This could inspire modern cyber law, which often struggles with gaps between novel crimes and existing regulations. For example, phishing or online data theft may be analogized to *jarīmah sariqah* but addressed through contextually appropriate *taʿzīr* penalties. Conversely, modern cyber law's use of digital evidence can enrich Islamic criminal procedure, as classical *fiqh* did not address digital forensics. Such integration would strengthen evidentiary standards in Islamic law without undermining its normative foundations (Goodman, 2020).

Another critical aspect is the transnational dimension of cybercrime. Classical Islamic law was territorially bound within states or caliphates, yet the universal principles of *sharīʿah* allow for global applicability. This universality resonates with the principle of Mutual Legal Assistance (MLA) in modern cyber law, which promotes international cooperation against cybercrime. Thus, Islamic criminal law can serve as a universal ethical framework, while modern law provides the procedural mechanisms for cross-jurisdictional enforcement (Bassiouni, 2014).

In Indonesia, integrating Islamic criminal law with modern cyber law is particularly significant. As the world's largest Muslim-majority nation and a member of the international

community, Indonesia faces the dual obligation to harmonize *sharīʿah* values with positive law. This is evident in the application of the ITE Law, which has often been criticized for over-criminalization and ambiguity. If evaluated through the lens of *maqāṣid al-sharīʿah*, the ITE Law could be refined not only in formal legal terms but also to ensure substantive justice and public welfare. Such integration would produce a legal system more responsive to technological change, rooted in local values, yet aligned with international standards (Nasution, 2020).

The practical implication of this comparative analysis is the necessity of developing a hybrid enforcement model that fuses Islamic criminal law and modern cyber law. This model could be institutionalized through national regulations that incorporate *sharīʿah* principles into sanction frameworks while adopting modern procedural and technical tools. For instance, the principle of *ḥifẓ al-māl* (protection of property) could reinforce personal data protection laws, while digital forensics and international cooperation mechanisms could ensure effective enforcement. Such a model represents not a compromise but an innovative effort to construct a legal system that is just, technologically relevant, and morally grounded. In this way, Islamic law and modern law should not be seen as adversarial systems but as complementary frameworks jointly addressing the challenges of digital globalization (Kuner, 2020).

Integrative Model of Law Enforcement

The concept of an integrative model of law enforcement in addressing cybercrime emerges from the awareness that digital crime cannot be resolved by relying solely on one legal approach. Islamic criminal law offers a moral–transcendental framework grounded in revelation, emphasizing responsibility, ethics, and the protection of the *maqāṣid al-sharīʿah*. Meanwhile, modern cyber law provides a systematic, procedural, and internationally connected regulatory framework. When placed in an integrative paradigm, these two models can complement one another and provide comprehensive answers to the increasingly complex challenges of digital crime.

The hybrid model serves as the key framework in this idea. A hybrid model seeks to combine the ethical values derived from *maqāṣid al-sharīʿah* with the regulatory instruments of modern cyber law. For instance, the principles of protecting property (*ḥifẓ al-māl*) and intellect (*ḥifẓ al-ʿaql*)—fundamental in Islamic law—can be used as ethical norms in drafting contemporary regulations. Modern cyber law, including international conventions on

cybercrime, already recognizes the importance of protecting digital consumers, personal data, and the right to privacy—values that are essentially consistent with the objectives of *maqāṣid al-sharī'ah*. Thus, the hybrid model bridges the gap between Islam's transcendental values and the operational mechanisms of positive law.

In this regard, one significant recommendation is strengthening regulation based on Islamic ethics. Modern regulations, particularly in Muslim-majority countries, should not merely adopt Western legal instruments but also incorporate Islamic ethics as a moral framework. For example, Indonesia's Electronic Information and Transactions Law (UU ITE) can be enriched with perspectives from *fiqh jināyah*, ensuring that sanctions are not only repressive but also educational and preventive, in line with the principle of *ta'zīr* in Islamic law. This is crucial so that law enforcement does not stop at the legal–formal aspect but also addresses the morality of offenders and the broader society (al-Qaradawi, 2001).

Another strategic component in this integrative model is Islamic digital literacy education. Digital crime often arises from weak ethical awareness among technology users, both individuals and institutions. Digital literacy based on Islamic ethics provides guidance for Muslims in using technology responsibly. This literacy is not limited to technical issues such as data security but also emphasizes values of honesty (*ṣidq*), trustworthiness (*amānah*), and prohibitions against fraud (*gharar*) and hacking that harm others. Thus, Islamic digital literacy becomes a preventive step aligned with *maqāṣid al-sharī'ah* in safeguarding social order in cyberspace (Kamali, 2008).

Another recommendation is to strengthen the role of contemporary fatwa councils and *qāḍī* in providing legal guidance on cybercrime cases. As is known, Islamic law has flexibility through *ijtihād*, which allows for the issuance of new fatwas in accordance with contemporary developments. Fatwa institutions can issue normative guidelines on social media conduct, online transactions, and digital security, providing society with both moral and legal reference points. At the judicial level, contemporary *qāḍī* can interpret new offenses through *siyāsah shar'iyyah*, thus addressing cybercrime cases absent from classical literature. In this way, Islamic law maintains its relevance amid technological modernization (al-Zuhayli, 1997).

Equally important, this integrative model should also be directed toward international synergy. Cybercrime is inherently transnational, making it impossible to address exclusively through national or religious legal systems. Hence, Muslim-majority countries could initiate international forums that blend Islamic legal perspectives with global

instruments such as the Budapest Convention on Cybercrime. Such forums could serve as platforms for intergovernmental dialogue, producing agreements grounded in *maqāṣid al-sharī'ah* while aligned with international legal needs. In doing so, Islamic law could contribute significantly at the global level, rather than remaining a particularistic system limited to national contexts.

The integrative model also responds to critiques that Islamic criminal law is rigid and irrelevant in modern contexts. Through this integrative approach, the flexibility of Islamic law—via *ta'zīr* and *siyāsah shar'iyyah*—can be combined with modern regulatory systems rich in procedural and technical instruments. Ultimately, the hybrid model aims to create a legal system that is not only repressive but also preventive, educative, and transformative. It not only punishes cybercriminals but also builds collective moral awareness within the digital society.

Thus, the integration between Islamic criminal law and modern cyber law can be seen as a harmonization between moral–transcendental values and technical–positivistic regulations. This harmonization aligns with the idea that law is not merely a tool for social control but also a moral instrument for maintaining human balance. In the context of cybercrime, this balance encompasses the protection of human rights, digital security, and the preservation of justice grounded in both sharī'ah and modern positive law (Rahman, 2019).

The integrative model of law enforcement cannot be separated from the dynamics between religious and state norms in regulating modern society. In the cybercrime context, integration is not only about merging two legal systems but also about building a new paradigm for understanding digital crime. Islamic criminal law emphasizes spirituality and vertical accountability to God, while modern cyber law focuses on procedure, legality, and intergovernmental cooperation. These two perspectives are complementary: Islamic law provides normative direction, while modern law provides implementation mechanisms. Therefore, their integration results in a comprehensive model of law enforcement, valid both legally and morally (An-Na'im, 2008).

One key advantage of integration is its ability to resolve the dilemma between legal certainty and substantive justice. Modern positive law often falls into proceduralism, making substantive justice difficult to achieve in some cases. Conversely, Islamic criminal law emphasizes substantive justice, although it sometimes lacks formal procedural instruments. By combining the two, legal systems can strike a balance between certainty and justice. For

example, in cases of online fraud, modern cyber law provides digital forensic procedures, while Islamic law adds a moral dimension by stressing accountability before God, ensuring offenders are not only punished but also directed toward repentance (al-Mawardi, 1996).

Furthermore, the integrative model can overcome the weaknesses of both systems. Modern cyber law struggles with moral authority, as its rules are often value-neutral and lack binding moral power in religious societies. Islamic criminal law provides a moral compass by grounding legal norms in transcendental values. Conversely, Islamic criminal law struggles with technical complexities in responding to highly sophisticated and transnational cybercrimes. Here, modern cyber law plays a critical role, offering standardized legal mechanisms at the international level, such as the Budapest Convention. Thus, integration is not merely a compromise but a strategic synergy (Kamali, 2019).

Another crucial aspect is the development of regulations based on *maqāṣid al-sharī'ah*. Modern cyber law typically rests on principles of human rights, legal certainty, and consumer protection. These principles align with *maqāṣid*, particularly *ḥifẓ al-'aql* (protection of intellect), *ḥifẓ al-māl* (protection of wealth), and *ḥifẓ al-'ird* (protection of honor). Using *maqāṣid* as an ethical framework ensures cyber regulations safeguard not only technical matters but also social harmony. For instance, regulations concerning the spread of hoaxes or hate speech online can be reinforced through the principle of *ḥifẓ al-'aql*, as false information damages public rationality and creates social discord (Shatibi, 1997).

On a practical level, this integrative model also underscores the importance of synergy between religious institutions, the state, and the international community. Fatwa councils and sharī'ah authorities can formulate Islamic ethical standards for digital activities. The state, through national legislation, enforces mechanisms, sanctions, and law enforcement coordination. Meanwhile, the international community ensures harmonization of cross-border regulations. This synergy strengthens the effectiveness of law enforcement since cybercrime is global and unconstrained by territorial boundaries. Hence, the integrative approach also promotes a fairer global digital governance based on universal values and religious ethics (Rahman, 2020).

In addition to strengthening regulations and institutions, Islamic digital literacy education is a preventive dimension that cannot be overlooked. The integrative model emphasizes that prevention is more important than prosecution. Islamic digital literacy goes beyond teaching technical skills, instilling moral awareness in digital engagement. For instance, campaigns on cyber ethics grounded in Islamic values can be integrated into

curricula and da'wah programs. This aligns with the principles of *ta'līm* and *tarbiyah* in Islam, which emphasize character building before punitive measures. If society develops ethical awareness, the space for digital crime will be significantly reduced (Fadlullah, 2015). Integration also offers new perspectives on the role of the contemporary *qāḍī*. In Islamic tradition, the *qāḍī* has the authority to interpret law in line with contemporary needs through *ijtihād*. In modern contexts, the *qāḍī* can collaborate with judges in national judicial systems to inject ethical and moral perspectives into cybercrime rulings. This collaboration strengthens legal legitimacy while ensuring justice is more holistic. For example, in cases of digital bank hacking, the *qāḍī* can stress the importance of *ḥifẓ al-māl* as a *maqāṣid* principle, while modern judges ensure procedural technicalities, such as digital forensic evidence, are met.

Ultimately, the integrative model also opens opportunities for developing a global Islamic legal framework in the digital age. If Muslim countries initiate international legal forums based on *maqāṣid*, Islam can contribute significantly to shaping global digital governance. This is crucial given today's challenges of cross-border cybercrime, massive data theft, and threats to digital sovereignty. By promoting *maqāṣid al-sharī'ah*, Islamic law can present itself as a normative framework emphasizing universal justice, transcendental ethics, and global social responsibility (Dusuki & Abdullah, 2007).

In conclusion, the integrative model of law enforcement against cybercrime is an effort to provide a holistic legal solution—one that addresses technical and procedural needs while strengthening moral, ethical, and spiritual dimensions. It answers the anxieties of modernity, which often neglects transcendental values in regulation, while also resolving the limitations of classical Islamic law in addressing new challenges. This hybrid model ultimately affirms that cyber law enforcement in the Muslim world must be based on *maqāṣid al-sharī'ah*, harmonized with practical and global modern legal instruments.

CONCLUSION

Cybercrime, as a phenomenon of modern law, reflects a complexity that demands a comprehensive response from various legal systems. From the perspective of positive law, cybercrime is regarded as a criminal act with transnational dimensions, requiring precise technical regulatory instruments such as the Budapest Convention and Indonesia's Electronic Information and Transactions Law (ITE Law). In Islamic criminal law, however, this phenomenon is closely related to the concept of *jarīmah*, particularly within the category

of *ta'zīr*, which allows flexibility in interpreting new offenses in line with changing circumstances. Thus, there is a meeting point between Islamic criminal law and modern positive law in terms of protecting society, preventing crime, and enforcing justice.

The model of Islamic criminal law enforcement can be integrated with modern cyber law through the approach of *maqāṣid al-sharī'ah*. The principles of protecting religion (*ḥifẓ al-dīn*), life (*ḥifẓ al-nafs*), intellect (*ḥifẓ al-'aql*), property (*ḥifẓ al-māl*), and honor (*ḥifẓ al-'irḍ*) align with the goals of modern regulations that emphasize digital security, human rights protection, and social order. This integration not only provides a strong normative framework but also enriches positive regulations with moral and transcendental values.

Therefore, it is crucial to develop an integrative framework that unites Islamic moral values with modern positive legal instruments. This framework may take the form of a hybrid model that emphasizes three key elements: first, strengthening regulations based on Islamic ethics; second, preventive Islamic digital literacy; and third, institutional synergy among fatwa councils, contemporary *qāḍīs*, national law enforcement authorities, and international forums. Through this integrative approach, law enforcement against cybercrime will not only be legally effective but also morally sound, thereby achieving substantive justice while maintaining order in cyberspace in the global era.

IMPLICATION

This article presents several significant implications at the academic, regulatory, and practical levels.

First, academic implications: This research opens new avenues for examining the relevance of Islamic criminal law in addressing contemporary phenomena such as cybercrime. Historically, Islamic law has often been perceived as limited to classical crimes. Yet through the category of *ta'zīr* and the *maqāṣid al-sharī'ah* approach, it demonstrates high flexibility in responding to digital crimes. Thus, this study enriches the discourse of modern Islamic law while bridging the gap between the tradition of *fiqh jināyah* and positive criminal law.

Second, regulatory implications: This article encourages policymakers to develop a hybrid legal model that integrates Islamic principles with modern cyber law instruments. Such integration is especially vital in Muslim-majority countries like Indonesia, which possess a strong moral-religious foundation while also being bound by international legal commitments. National regulations such as the ITE Law can be enriched with the *maqāṣid*

framework, ensuring that sanctions are not only deterrent in nature but also ethically and socially constructive.

Third, practical implications: A key implication of this study is the need to strengthen Islamic digital literacy. Preventive measures rooted in value-based education are essential for reducing cybercrime from an early stage. This can be realized through the integration of educational curricula, da'wah programs, and public policies that emphasize ethical use of technology. On the other hand, law enforcement officers and contemporary *qāḍīs* can collaborate to ensure that legal rulings are not only legally just but also morally and transcendentally valid.

Fourth, global implications: This article highlights the necessity of an international forum that brings together the perspective of Islamic law with modern legal instruments such as the Budapest Convention. In doing so, Muslim-majority countries can contribute to building a more just global digital governance system, grounded in universal values and the transcendental ethics of Islam.

Overall, the main implication of this research is that cybercrime law enforcement cannot rely on a single legal system. Instead, an integrative framework is needed to unite the strengths of Islamic criminal law and modern cyber law, thereby producing a more comprehensive, effective, and just cyber legal order in addressing the challenges of the digital age.

BIBLIOGRAPHY

Abū Zahrah, Muḥammad. 2021. *'Ilm al-Jarā'im wa al-'Uqūbāt*. Kairo: Dār al-Fikr al-'Arabī.

Abū Zahrah, Muḥammad. 2021. *Uṣūl al-Fiqh*. Kairo: Dār al-Fikr al-'Arabī.

Ahmed, A. (2021). "Islamic Criminal Law and Cybercrime: Exploring Ta'zir Sanctions in the Digital Age." *Journal of Islamic Law and Ethics*, 12(2).

Al-Ashqar, 'Umar Sulaimān. 2023. *Jarīmah al-Ḥadīthah wa Mawqif al-Sharī'ah minhā*. Amman: Dār al-Nafā'is.

Al-Bannā, Ḥasan. 2021. *Mabādi' al-Sharī'ah wa Naẓariyyātuhā*. Kairo: Dār al-Salām.

Ali, Zainuddin. 2021. *Hukum Pidana Islam*. Jakarta: RajaGrafindo Persada.

Al-Jazīrī, 'Abd al-Raḥmān. 2020. *Kitāb al-Fiqh 'alā al-Madhāhib al-Arba'ah*. Kairo: Dār al-Fikr.

Al-Kāsānī. 2020. *Badā'i' al-Ṣanā'i' fī Tartīb al-Sharā'i'*. Beirut: Dār al-Kutub al-'Ilmiyyah.

Al-Māwardī, Abū al-Ḥasan. 2021. *Al-Aḥkām al-Sulṭāniyyah*. Beirut: Dār al-Kutub al-'Ilmiyyah.

Al-Qaradawi, Yusuf. 2020. *Fiqh al-Jarīmah wa al-'Uqūbah*. Kairo: Maktabah Wahbah.

Al-Shāṭibī, Abū Isḥāq. 2021. *Al-Muwāfaqāt fī Uṣūl al-Sharī'ah*. Beirut: Dār al-Ma'rifah.

Al-Ṭabarī. 2021. *Jāmi' al-Bayān fī Tafsīr al-Qur'ān*. Beirut: Dār al-Ma'rifah.

Al-Zuḥaylī, Wahbah. 2020. *Al-Fiqh al-Islāmī wa Adillatuhū*. Damaskus: Dār al-Fikr.

Anwar, Syamsul. 2021. *Hukum Islam Kontemporer*. Jakarta: Kencana.

Arief, Barda Nawawi. 2020. *Bunga Rampai Kebijakan Hukum Pidana*. Jakarta: Kencana.
Asshiddiqie, Jimly. 2022. *Hukum dan Teknologi Informasi*. Jakarta: Konstitusi Press.
Atmasasmita, Romli. 2021. *Sistem Peradilan Pidana*. Bandung: Mandar Maju.
Auda, Jasser. 2008. *Maqasid al-Shariah as Philosophy of Islamic Law: A Systems Approach*. London: IIIT.
Auda, Jasser. 2010. *Maqasid al-Shariah: A Beginner's Guide*. London: IIIT.
Bassiouni, M. Cherif. 2014. *Introduction to International Criminal Law*. Leiden: Brill.
Bassiouni, M. Cherif. 2021. *International Criminal Law and Cybercrime*. Leiden: Brill.
Brenner, Susan W. 2010. *Cybercrime: Criminal Threats from Cyberspace*. Santa Barbara: Praeger.
Brenner, Susan W. 2021. *Cybercrime and the Law: Challenges of the 21st Century*. New York: Routledge.
Busyro. 2022. *Hukum Siber di Indonesia: Analisis Kritis UU ITE*. Jakarta: Prenada Media.
Castells, Manuel. 2020. *The Internet Galaxy*. Oxford: Oxford University Press.
Chazawi, Adami. 2021. *Hukum Pidana Positif di Indonesia*. Jakarta: RajaGrafindo Persada.
Clough, Jonathan. 2015. *Principles of Cybercrime*. Cambridge: Cambridge University Press.
Clough, Jonathan. 2021. *Principles of Cybercrime*. Cambridge: Cambridge University Press.
Djamil, Fathurrahman. 2020. *Filsafat Hukum Islam*. Jakarta: Logos.
Esposito, John L., & Natana J. DeLong-Bas. 2018. *Shariah: What Everyone Needs to Know*. Oxford: Oxford University Press.
Fitriani, N., & Ramadhan, Y. (2022). "Penegakan Hukum Terhadap Cybercrime di Indonesia: Tinjauan UU ITE dan Fiqh Jinayah." *Jurnal Hukum Islam Indonesia*, 14(1),
Goodman, Marc. 2020. *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*. New York: Anchor Books.
Hallaq, Wael B. 2009. *Shari'a: Theory, Practice, Transformations*. Cambridge: Cambridge University Press.
Hamzah, Andi. 2020. *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta.
Haryadi, Dwi. 2023. *Tindak Pidana Siber dan Penegakan Hukumnya di Indonesia*. Bandung: Refika Aditama.
Hiariej, Eddy OS. 2020. *Prinsip-Prinsip Hukum Pidana*. Jakarta: Erlangga.
Holt, Thomas J. 2022. *Cybercrime and Digital Forensics: An Introduction*. London: Routledge.
Hunter, David. 2021. *Cyberspace Law: Cases and Materials*. New York: Aspen Publishers.
Hussain, M. (2023). "Cybersecurity and Maqāṣid al-Sharī'ah: An Integrative Approach." *International Journal of Cyber Law and Islamic Studies*, 5(3),
Ibn Qayyim al-Jawziyyah. 2022. *Al-Ṭuruq al-Ḥukmiyyah fī al-Siyāsah al-Shar'iyyah*. Kairo: Dār al-Ḥadīth.
Ibn Taymiyyah. 2021. *Al-Siyāsah al-Shar'iyyah*. Riyadh: Maktabah al-Rushd.
Jahar, Asep Saepudin. 2020. *Hukum Islam dan Transformasi Sosial*. Jakarta: Kencana.
Kamali, Mohammad Hashim. 2019. *Shari'ah Law: An Introduction*. Oxford: Oneworld.
Kerr, Orin S. 2021. *Computer Crime Law*. St. Paul: West Academic Publishing.
Khallaf, Abdul Wahhab. 2020. *'Ilm Uṣūl al-Fiqh*. Kairo: Maktabah Da'wah.
Kuner, Christopher. 2020. *Transborder Data Flows and Data Privacy Law*. Oxford: Oxford University Press.
Lessig, Lawrence. 2020. *Code and Other Laws of Cyberspace*. New York: Basic Books.
Loader, Brian. 2020. *The Governance of Cyberspace*. London: Routledge.
Mudzhar, M. Atho. 2020. *Pendekatan Studi Islam*. Yogyakarta: Pustaka Pelajar.
Muhammad, Husein. 2022. *Fiqh Perempuan*. Yogyakarta: LKiS.

Muladi. 2020. *Kapita Selekta Hukum Pidana*. Semarang: UNDIP Press.
Muslich, Ahmad Wardi. 2020. *Hukum Pidana Islam*. Jakarta: Sinar Grafika.
Nasution, Adi. 2020. *Hukum Siber di Indonesia: Analisis UU ITE dan Tantangan Penegakan Hukum*. Jakarta: Kencana.
Poernomo, Bambang. 2021. *Asas-Asas Hukum Pidana Islam dan Penerapannya*. Yogyakarta: Liberty.
Prasetyo, Teguh. 2023. *Hukum Pidana dalam Perspektif Cyber Crime*. Bandung: Nusa Media.
Putra, R., & Suryadi, D. (2021). "Kejahatan Siber dalam Perspektif Hukum Pidana Islam." *Al-Ahkam: Jurnal Ilmu Syari'ah dan Hukum*, 31(2
Qal'ahjī, Muḥammad Rawwās. 2020. *Al-Mu'jam al-Fiqhī*. Beirut: Dār al-Nafā'is.
Rahardjo, Satjipto. 2020. *Hukum dan Perubahan Sosial*. Jakarta: Genta Publishing.
Saeed, A. (2024). "The Budapest Convention and Its Applicability in Muslim Countries." *Journal of International Cyber Law*, 19(1),
Santoso, B. (2022). "Cybercrime dan Tantangan Penegakan Hukum di Indonesia." *Jurnal Hukum dan Teknologi*, 7(2),
Setiadi, Edi. 2021. *Hukum Pidana Islam: Sebuah Pengantar*. Bandung: Refika Aditama.
Sieber, Ulrich. 2021. *Legal Aspects of Cybercrime*. Strasbourg: Council of Europe Publishing.
Solove, Daniel J. 2021. *Understanding Privacy in the Digital Age*. Stanford: Stanford University Press.
Susskind, Richard. 2021. *Tomorrow's Lawyers: An Introduction to Your Future*. Oxford: Oxford University Press.
UNODC. *Comprehensive Study on Cybercrime*. Vienna: United Nations Office on Drugs and Crime, 2019.
Wahyuni, R. (2020). "Maqashid al-Syari'ah dan Perlindungan Data Pribadi di Era Digital." *Jurnal Al-Mazahib*, 8(1),
Wall, David. 2020. *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity.
Yar, Majid. 2022. *Cybercrime and Society*. London: SAGE.
Yusoff, M. (2023). "Islamic Legal Response to Cyber Fraud: A Comparative Study." *Malaysian Journal of Syariah and Law*, 31(4),
Zubair, A. (2025). "Hybrid Model of Cyber Law Enforcement: Islamic and Modern Perspectives." *Journal of Law, Technology and Society*, 15(2),
Zulkifli, H. (2021). "Ta'zir and Cybercrime: Reconstructing Islamic Criminal Law in the Digital Age." *Al-Jinayah: Jurnal Hukum Pidana Islam*