ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

CYBER CRIMES AND THEIR LEGAL STATUS: A COMPARATIVE STUDY BETWEEN ISLAMIC LAW AND INTERNATIONAL LAW

Dr Hafiz Muhammad Arif Siddiqi
Visiting Lecturer
Department of Islamic Studies Government College University Faisalabad, Punjab
marisiddiqi@gcuf.edu.pk
Immad Uddin Ahmed
PhD Scholar
LECTURER
Department of Sciences & Humanities
FAST NUCES KARACHI
immad.ahmed@nu.edu.pk
Syed Abrar Hussain Shah
Humanities Department,
COMSATS University Islamabad, Vehari Campus
abrarhussain@cuivehari.edu.pk

Abstract:

In the contemporary era, the rapid expansion of the digital revolution and information technologies has profoundly transformed human society, economy, and legal systems. As a consequence of these developments, a new dimension of criminal activity has emerged, commonly referred to as "cyber crimes." These offenses transcend traditional geographical boundaries and operate on a global scale, characterized by speed, anonymity, and increasing complexity. In this context, legal systems face a fundamental challenge in defining, classifying, and effectively regulating these emerging forms of crime within coherent legal frameworks.This study provides a comparative analysis of the legal status of cyber crimes within the frameworks of Islamic law and international law. In the Islamic legal tradition, the concept of crime is deeply rooted in ethical and spiritual principles, where the objectives of Shariah Hifz al-Din (protection of religion), Hifz al-Nafs (protection of life), Hifz al-Mal (protection of wealth), Hifz al-Aql (protection of intellect), and Hifz al-Ird (protection of dignity) serve as foundational pillars. Within this framework, cyber crimes are generally addressed under the discretionary category of Ta'zir, allowing flexible and context-based legal responses. In contrast, international legal systems regulate cyber crimes primarily through statutory laws, conventions, and treaty-based frameworks, including instruments such as the Budapest Convention and the General Data Protection Regulation (GDPR).

The paper critically examines the theoretical, doctrinal, and practical dimensions of both legal systems. It highlights the ethical and objective-based (Maqasid-oriented) approach of Islamic law and explores its compatibility with modern legal requirements. At the same time, it analyzes key challenges within international law, including jurisdictional conflicts, admissibility of digital evidence, and limitations in cross-border enforcement mechanisms.The overall findings indicate that although Islamic and international legal systems differ in their philosophical foundations and structural design, both share a common objective: the protection of human rights, the establishment of justice, and the maintenance of social order. Therefore, the study emphasizes the need for a more integrated legal framework capable of addressing the evolving challenges of the digital age.

Keywords: Cyber Crimes, Islamic Law, International Law, Comparative Legal Study, Maqasid al-Shariah, Cyber Security, Digital Justice, Transnational Crime, Data Protection, Jurisdictional Issues

Theoretical and Conceptual Foundations of Cyber Crimes

Concept of Cyber Crime in Modern Legal Systems

Cyber crime has become a central concern in contemporary legal systems due to the rapid expansion of digital technologies and global internet connectivity. Modern societies increasingly depend on information systems for communication, finance, governance, education, and security.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

This dependency has given rise to new forms of criminal activity that operate in virtual environments rather than physical spaces. Cyber crime generally refers to unlawful acts committed through computers, digital devices, or networks, including hacking, identity theft, online financial fraud, data breaches, cyber stalking, and digital espionage. Modern legal systems have therefore developed specialized cyber laws to address issues such as jurisdiction, electronic evidence, and cross-border enforcement challenges.

Ibn Khaldun states:

"الظلم مؤذن بخراب العمران، وإذا انتشر الفساد في المعاملات اختل نظام الدولة[1]".

"Injustice leads to the destruction of civilization, and when corruption spreads in transactions, the order of the state is disrupted."

Ibn Khaldun's sociological insight, though formulated in a pre-digital context, provides a powerful conceptual lens for understanding cyber crime today. Cyber offenses such as digital fraud, hacking of financial systems, and manipulation of online transactions represent a modern form of corruption in human dealings. These acts undermine trust in digital infrastructure, weaken institutional credibility, and disrupt economic and social stability. In this sense, cyber crime can be interpreted as a contemporary manifestation of the broader principle of social decay caused by systemic injustice and corruption.

Nature and Scope of Cyber Crimes in the Digital Age

The nature of cyber crime in the digital age is defined by its borderless, anonymous, and rapidly evolving characteristics. Unlike traditional crimes that are limited by geography and physical presence, cyber crimes can be committed remotely across multiple jurisdictions within seconds. The scope of cyber crime extends to individuals, private organizations, financial institutions, and state infrastructures. It includes offenses such as unauthorized access to systems, malware attacks, ransomware, online harassment, intellectual property theft, digital terrorism, and large-scale data breaches. As technology advances, cyber criminals continuously develop more sophisticated methods, making cyber crime one of the most dynamic challenges for modern legal systems.Al-Ghazali states:

"العدل أساس الملك، وإذا ضاع العدل ضاعت الحقوق وتفرقت الجماعة[2]".

"Justice is the foundation of governance, and when justice is lost, rights are destroyed and society becomes divided."

Al-Ghazali's principle emphasizes the foundational role of justice in maintaining social order. In the context of the digital age, cyber crimes represent a direct threat to this principle by violating privacy, disrupting financial systems, and undermining trust in digital governance. When digital systems are compromised, individuals lose confidence in institutions, and societal stability is weakened. Thus, cyber crime is not merely a technical violation but a profound disruption of justice and order in modern digital societies.

Cyber crime in modern legal systems represents a complex intersection of technology, law, and ethics. Its borderless nature and rapid evolution challenge traditional legal frameworks and demand continuous adaptation of regulatory mechanisms. While modern cyber laws address

[1] Ibn Khaldun, 'Abd al-Rahman ibn Muhammad. Al-Muqaddimah. Beirut: Dar al-Fikr, 2004, Vol. 1, p. 348.

[2] Al-Ghazali, Abu Hamid Muhammad ibn Muhammad. Ihya' 'Ulum al-Din. Cairo: Dar al-Hadith, 1999, Vol. 2, p. 87.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

technical and procedural aspects of these crimes, classical ethical and sociological insights highlight the deeper consequences of corruption and injustice. Together, these perspectives demonstrate that cyber crime is not only a legal issue but also a broader social and moral challenge that threatens trust, security, and stability in both digital and physical societies.

Classification of Cyber Crimes (Traditional and Modern Forms)

Cyber crimes can be classified on the basis of their nature, target, and technological execution. In modern legal systems, cyber crimes are generally divided into traditional forms that have migrated into the digital environment and modern forms that exist exclusively due to technological advancement. Traditional forms include fraud, theft, blackmail, and forgery, now executed through digital platforms such as emails, social media, and online banking systems. Modern cyber crimes, on the other hand, include hacking, ransomware attacks, phishing, identity theft, cyber terrorism, data breaches, deepfake manipulation, and attacks on critical infrastructure. This classification helps legal systems to design appropriate preventive, investigative, and punitive mechanisms suited to the evolving nature of digital offenses.Imam Al-Mawardi states:

"إن المقصود من السياسة حفظ الدين والدنيا، وردع الظالم، وإنصاف المظلوم[3]".

"The purpose of governance is the protection of religion and worldly affairs, restraining the oppressor, and ensuring justice for the oppressed."

Al-Mawardi's principle reflects the foundational objective of law enforcement, which is highly relevant in the classification of cyber crimes. Whether traditional or modern, all forms of cyber crime represent violations of justice and security. The digital transformation of criminal behavior requires governance systems to extend their protective mechanisms into cyberspace. Thus, cyber crime classification is not merely a technical exercise but part of a broader legal and ethical responsibility to maintain justice and social order.

Concept of Crime (Jarimah) in Islamic Criminal Law

In Islamic criminal law, the concept of crime is referred to as Jarimah, which encompasses any act that violates the rights of Allah, the rights of individuals, or public order as defined by Shari'ah. Islamic jurisprudence classifies crimes into three major categories: Hudud (fixed punishments), Qisas (retaliation-based offenses), and Ta'zir (discretionary punishments). The concept of Jarimah is rooted in moral accountability, social justice, and the preservation of fundamental human interests, including religion, life, intellect, lineage, and property. In the context of cyber space, many digital offenses can be analyzed under the category of Ta'zir, as they involve harm without fixed classical legal precedents.Imam Al-Shatibi states:

"الشريعة إنما وضعت لمصالح العباد في الدنيا والآخرة[4]".

"The Shari'ah has been established only for the welfare of human beings in this world and the hereafter."

Al-Shatibi's statement highlights the objective-based nature of Islamic law (Maqasid al-Shari'ah). The concept of Jarimah is therefore not limited to rigid legal definitions but extends to any act that disrupts human welfare. Cyber crimes, such as digital fraud, identity theft, and online exploitation, fall under this broader understanding because they harm individuals and society.

[3] Al-Mawardi, Abu al-Hasan Ali ibn Muhammad. Al-Ahkam al-Sultaniyyah. Cairo: Dar al-Hadith, 2001, p. 112.

[4] Al-Shatibi, Ibrahim ibn Musa. Al-Muwafaqat fi Usul al-Shari'ah. Beirut: Dar al-Kutub al-'Ilmiyyah, 2003, Vol. 2, p. 15.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

Islamic criminal law thus provides a flexible framework that can accommodate new forms of crime while maintaining its ethical foundation.

Comparative Study of Crime in Islamic and International Law

A comparative analysis of crime in Islamic and international law reveals both convergence and divergence in legal philosophy and application. International law defines crime primarily in terms of statutory violations, state sovereignty, and human rights frameworks, while Islamic law defines crime through moral, legal, and spiritual dimensions grounded in divine guidance. International legal systems emphasize codified statutes, procedural justice, and state enforcement, whereas Islamic law integrates ethical accountability with legal sanctions. Despite these differences, both systems aim to protect human dignity, ensure justice, and maintain social order. In the context of cyber crime, both legal traditions face the shared challenge of regulating borderless digital offenses and ensuring effective enforcement mechanisms.Imam Ibn Taymiyyah states:

"إن العدل واجب على كل أحد، وبه تقوم السماوات والأرض[5]".

"Justice is obligatory upon everyone, and by it the heavens and the earth are sustained."

Ibn Taymiyyah's statement underscores justice as a universal principle that transcends legal systems. In both Islamic and international law, justice serves as the foundation for criminal regulation. Cyber crimes challenge this principle by undermining trust, security, and fairness in digital interactions. A comparative legal framework shows that while methodologies differ, the ultimate objective remains the same: protection of rights and establishment of justice. This shared ethical foundation provides opportunities for legal convergence in addressing global cyber threats.

The classification of cyber crimes, the Islamic concept of Jarimah, and the comparative analysis between Islamic and international legal systems collectively demonstrate the evolving nature of criminal law in the digital age. While international law provides structured regulatory mechanisms, Islamic law offers a deeply ethical and objective-based framework. Together, these perspectives contribute to a more comprehensive understanding of cyber crime, emphasizing justice, protection of rights, and adaptability to emerging technological realities.

Legal Framework of Cyber Crimes in International Law

Historical Development of Cyber Law in International Systems

The historical development of cyber law in international systems is closely linked to the rapid expansion of information and communication technologies during the late twentieth century. As computer networks began to connect individuals, institutions, and governments across borders, new legal challenges emerged that traditional criminal law frameworks were not designed to address. Early concerns focused on unauthorized access, data theft, and computer fraud, which gradually evolved into more complex forms of cyber crime such as hacking networks, digital espionage, and large-scale cyber warfare.

During the 1980s and 1990s, states and international organizations began recognizing the need for specialized legal instruments to regulate cyberspace. This led to the development of national cyber laws and regional agreements, followed by broader international cooperation initiatives. The Council of Europe's Budapest Convention on Cybercrime (2001) is widely regarded as the first comprehensive international treaty addressing cyber crime, establishing standards for harmonizing

[5] Ibn Taymiyyah, Ahmad ibn Abd al-Halim. Majmu' al-Fatawa. Riyadh: King Fahd Complex, 1995, Vol. 28, p. 146.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

legislation, improving investigative cooperation, and strengthening procedural mechanisms for electronic evidence.

Imam Al-Shatibi states:

"الوسائل لها أحكام المقاصد، فإذا تغيرت الوسائل تغيرت كيفية التطبيق[6]".

"Means take the rulings of their objectives, and when means change, the method of application also changes."

Al-Shatibi's principle is highly relevant to the evolution of cyber law. The transition from physical crimes to digital offenses represents a fundamental change in the "means" through which criminal activity is conducted. Therefore, legal systems must adapt their mechanisms of enforcement and regulation accordingly. Cyber law emerges as a necessary adaptation of traditional legal principles to new technological realities. This demonstrates that while objectives of law justice, protection, and security remain constant, their implementation must evolve in response to technological transformation.

United Nations and Global Cyber Security Policies

The United Nations has played a significant role in shaping global responses to cyber security threats and cyber crime. As cyberspace transcends national boundaries, international cooperation becomes essential for ensuring security, stability, and lawful use of digital technologies. The UN has facilitated discussions on information security through its Group of Governmental Experts (GGE), which has issued multiple reports emphasizing norms of responsible state behavior in cyberspace. These include principles such as non-intervention, respect for sovereignty, and the prohibition of malicious cyber activities targeting critical infrastructure.

In addition to policy frameworks, the UN has encouraged capacity building in developing countries, promoting digital resilience, cybersecurity awareness, and legal harmonization across member states. Agencies such as the International Telecommunication Union (ITU) also contribute to global cyber security strategies by providing technical support, policy guidelines, and international coordination mechanisms.Ibn Khaldun states:

"إن الدولة إذا ضعفت فيها العصبية اختل نظامها وانهارت قوتها[7]".

"When solidarity within a state weakens, its system becomes disordered and its power declines."

Although Ibn Khaldun's concept of 'asabiyyah (social cohesion) was developed in a pre-digital era, it is highly applicable to global cyber security governance. In the modern context, cyber security requires strong international cooperation and collective responsibility among states. Weak coordination between nations leads to vulnerabilities in cyberspace, including cyber attacks, misinformation campaigns, and transnational cyber crime. Therefore, global cyber security policies function as a modern form of international solidarity necessary to maintain digital stability and collective security.

The historical development of cyber law and the role of the United Nations in cyber security governance demonstrate the gradual institutionalization of legal frameworks in response to digital transformation. While early cyber law focused on technical offenses, modern

[6] Al-Shatibi, Ibrahim ibn Musa. Al-Muwafaqat fi Usul al-Shari'ah. Beirut: Dar al-Kutub al-'Ilmiyyah, 2003, Vol. 2, p. 302.

[7] Ibn Khaldun, 'Abd al-Rahman ibn Muhammad. Al-Muqaddimah. Beirut: Dar al-Fikr, 2004, Vol. 1, p. 271.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

international systems emphasize cooperation, harmonization, and collective security. These developments reflect the necessity of adapting legal principles to technological change while maintaining core values of justice, security, and global stability in cyberspace.

Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime (2001), adopted by the Council of Europe, is widely regarded as the first comprehensive international treaty addressing cyber crime. It provides a harmonized legal framework for criminalizing core cyber offenses, establishing procedural powers for investigation, and enhancing international cooperation in combating cyber threats. The Convention covers offenses such as illegal access, data interference, system interference, computer-related fraud, and content-related crimes. It also introduces procedural tools like expedited preservation of electronic data and real-time collection of traffic data, which are essential in digital investigations.

One of the most significant aspects of the Budapest Convention is its emphasis on cross-border cooperation, recognizing that cyber crimes often transcend national jurisdictions and require coordinated international responses. It has influenced national legislation across many countries by providing a model framework for drafting cybercrime laws and mutual legal assistance mechanisms.

Imam Al-Ghazali states:

"إن النظام لا يقوم إلا بالعدل، وإذا فُقد العدل فسد الحكم وانهارت السياسة[8]".

"Order cannot be established except through justice, and when justice is lost, governance is corrupted and politics collapses."

Al-Ghazali's principle reflects the foundational importance of justice in governance systems. The Budapest Convention similarly aims to establish a form of "digital justice" by creating uniform legal standards to combat cyber crime. Without harmonized international legal frameworks, cyber criminals exploit jurisdictional gaps and legal inconsistencies. Thus, the Convention represents an attempt to restore order and justice in cyberspace by ensuring that states cooperate effectively against digital threats.

Digital Privacy and Data Protection Laws

Digital privacy and data protection laws have become a central component of international cyber legal frameworks due to the exponential growth of personal data collection and processing. With the rise of social media platforms, e-commerce systems, cloud computing, and artificial intelligence, vast amounts of sensitive personal data are continuously collected, stored, and analyzed. This has raised serious concerns regarding privacy violations, unauthorized data sharing, identity theft, and surveillance abuses.Legal systems have responded by introducing comprehensive data protection regulations such as the European Union's General Data Protection Regulation (GDPR), which establishes strict rules on consent, data processing, user rights, and corporate accountability. These laws aim to ensure transparency, safeguard individual privacy, and impose legal obligations on organizations handling personal data.

Ibn Taymiyyah states:

"الحقوق لا تُحفظ إلا بالعدل، والعدل أساس قيام المجتمع[9]".

[8] Al-Ghazali, Abu Hamid Muhammad ibn Muhammad. Ihya' 'Ulum al-Din. Cairo: Dar al-Hadith, 1999, Vol. 2, p. 87.

[9] Ibn Taymiyyah, Ahmad ibn Abd al-Halim. Majmu' al-Fatawa. Riyadh: King Fahd Complex, 1995, Vol. 28, p. 146.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

"Rights are not preserved except through justice, and justice is the foundation of societal existence."

Ibn Taymiyyah's statement highlights the essential relationship between justice and the protection of rights. In the digital age, privacy is a fundamental right that must be safeguarded through robust legal frameworks. Data protection laws reflect this principle by ensuring that individuals retain control over their personal information. Without such protections, digital systems become vulnerable to exploitation, undermining trust in technological governance and weakening societal stability.

Jurisdictional Issues in Cross-Border Cyber Crimes

Jurisdictional challenges represent one of the most complex aspects of international cyber law. Unlike traditional crimes, cyber crimes are not confined to a single geographical location; they often involve perpetrators, victims, and servers located in different countries. This creates significant legal difficulties in determining which state has jurisdiction, which laws apply, and how enforcement should be carried out.

Issues such as conflicting national laws, lack of extradition agreements, and differences in legal definitions of cyber offenses further complicate prosecution efforts. International cooperation mechanisms, including mutual legal assistance treaties (MLATs) and extradition agreements, are essential but often slow and limited in effectiveness. As a result, cyber criminals frequently exploit jurisdictional gaps to avoid prosecution.Imam Al-Mawardi states:

"السلطة لا تستقيم إلا بوحدة النظام، وإذا تعددت الجهات ضعفت القوة[10]".

"Authority cannot be stable except through unity of system, and when authorities are divided, power becomes weak."

Al-Mawardi's insight is directly applicable to jurisdictional issues in cyber crime. Fragmented legal systems and inconsistent jurisdictional rules weaken the ability of states to effectively combat cyber threats. In cyberspace, where crimes are inherently transnational, unity in legal frameworks and cooperation between jurisdictions is essential. Without coordination, enforcement becomes ineffective, allowing cyber criminals to operate across borders with minimal risk.

The Budapest Convention, digital privacy laws, and jurisdictional frameworks collectively represent the core structure of international cyber law. While significant progress has been made in harmonizing legal responses, challenges remain due to the borderless nature of cyberspace and differences in national legislation. Effective regulation of cyber crime requires continuous international cooperation, legal harmonization, and adaptation to technological advancements to ensure justice, security, and the protection of digital rights globally.

Cyber Crimes in Islamic Criminal Law

Protection of Life, Property, and Honour in Shariah

Islamic criminal law is fundamentally grounded in the protection of essential human interests (Maqasid al-Shari'ah), among which the safeguarding of life (Hifz al-Nafs), property (Hifz al-Mal), and honour (Hifz al-'Ird) occupies a central position. These protections are not merely legal provisions but are deeply rooted ethical and spiritual objectives designed to preserve human dignity and social order. In the context of modern digital environments, these principles extend naturally to cyber space, where threats to life, wealth, and reputation can occur through

[10] Al-Mawardi, Abu al-Hasan Ali ibn Muhammad. Al-Ahkam al-Sultaniyyah. Cairo: Dar al-Hadith, 2001, p. 112.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

digital means such as cyberbullying, financial fraud, identity theft, doxxing, and online defamation.

Islamic jurisprudence recognizes that harm (darar) is to be removed in all its forms, whether physical or virtual. Therefore, any cyber activity that endangers human dignity, compromises financial security, or violates personal privacy is considered a serious breach of Shariah objectives and falls under the scope of legal and ethical accountability.

Imam Al-Shatibi states:

"المقاصد الشرعية إنما وضعت لحفظ مصالح العباد في الدين والدنيا معا[11]".

"The objectives of Shariah were established to preserve the welfare of human beings in both religious and worldly affairs."

Al-Shatibi's statement highlights the comprehensive and purpose-driven nature of Islamic law. The protection of life, property, and honour is not limited to physical harm but extends to all forms of harm that threaten human welfare. In the digital age, cyber crimes such as hacking personal accounts, spreading false information, or stealing financial data directly violate these objectives. Therefore, Shariah-based legal reasoning can be extended to cyberspace, ensuring that modern technological harms are addressed within the ethical and legal framework of Islam.

Hirabah and Its Application to Digital Terrorism

The concept of Hirabah in Islamic criminal law refers to acts of public disorder, armed robbery, intimidation, and violent disruption of societal security. Traditionally, it is associated with crimes that spread fear, instability, and harm to individuals and communities. In the modern context, scholars have extended the conceptual framework of Hirabah to include digital terrorism and cyber warfare, where similar objectives are achieved through technological means rather than physical violence.

Digital terrorism includes cyber attacks on critical infrastructure, online radicalization, hacking of governmental systems, disruption of financial networks, and spreading fear through coordinated cyber operations. These acts mirror the essence of Hirabah because they create widespread insecurity, destabilize public order, and threaten national and global stability.Imam Ibn Taymiyyah states:

"الحرابة هي إفساد في الأرض بإخافة الناس وسلب أمنهم[12]".

"Hirabah is corruption on earth through instilling fear among people and depriving them of security."

Ibn Taymiyyah defines Hirabah as a crime that fundamentally undermines public safety and social order. In the digital era, cyber terrorism achieves the same objective through non-physical means. Cyber attackers who disrupt hospitals, financial systems, or government databases effectively create fear and instability similar to traditional Hirabah. Therefore, applying this classical concept to digital terrorism provides a strong jurisprudential foundation for addressing modern cyber threats within Islamic criminal law.

The principles of Shariah regarding the protection of life, property, and honour provide a comprehensive ethical and legal framework that naturally extends to cyberspace. Similarly, the

[11] Al-Shatibi, Ibrahim ibn Musa. Al-Muwafaqat fi Usul al-Shari'ah. Beirut: Dar al-Kutub al-'Ilmiyyah, 2003, Vol. 2, p. 18.

[12] Ibn Taymiyyah, Ahmad ibn Abd al-Halim. Majmu' al-Fatawa. Riyadh: King Fahd Complex, 1995, Vol. 28, p. 112.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

concept of Hirabah offers a powerful juristic foundation for understanding and addressing digital terrorism. Together, these principles demonstrate that Islamic criminal law is adaptable and capable of addressing modern cyber threats while preserving its core objectives of justice, security, and human dignity.

Financial Crimes: Theft, Fraud, and Online Scams

Financial crimes in cyberspace represent one of the most rapidly expanding categories of modern cyber offenses. These include digital theft, online fraud, phishing scams, credit card fraud, identity-based financial manipulation, and unauthorized access to banking systems. In Islamic criminal law, the protection of wealth (Hifz al-Mal) is a fundamental objective of Shariah, and any unlawful acquisition of another person's property is strictly prohibited. The transition of financial transactions into digital platforms has not altered the ethical and legal principles of Islam; rather, it has expanded their application into new technological contexts.

Islamic jurisprudence emphasizes transparency, honesty, and mutual consent in financial dealings. Therefore, any cyber activity that involves deception, misrepresentation, or unlawful appropriation of wealth is considered a serious violation of Shariah principles and falls under criminal liability.

Imam Al-Ghazali states:

"أكل أموال الناس بالباطل من أعظم أنواع الظلم[13]".

"Consuming people's wealth unlawfully is one of the greatest forms of injustice."

Al-Ghazali's statement highlights the moral severity of financial injustice. In the digital age, online fraud and cyber theft represent modern manifestations of consuming wealth unjustly. Whether through hacking bank accounts or manipulating online transactions, the essence of the crime remains the same: unlawful appropriation of property. Islamic law therefore extends its prohibition to all forms of financial misconduct, including digital environments, reinforcing the protection of economic justice and trust in society.

Privacy and Ethical Boundaries (Satr and Sanctity)

Privacy (Satr) and sanctity of personal life are deeply embedded ethical principles in Islamic teachings. Islam strictly prohibits the violation of private spaces, surveillance without justification, and exposure of personal faults. In the digital world, these principles extend to data privacy, online surveillance, unauthorized access to personal accounts, and the exposure of private information through hacking or social media platforms.

The ethical boundaries in Islam emphasize respect for human dignity and the protection of personal secrets. Cyber activities such as spying on individuals, leaking private data, and digital defamation directly contradict these principles and are considered violations of both moral and legal obligations.

The Qur'an states:

"وَلَا تَجَسَّسُوا وَلَا يَغْتَب بَّعْضُكُم بَعْضًا[14]"

"And do not spy on one another, nor backbite each other."

This Qur'anic principle establishes a clear prohibition against invading privacy and spreading personal information. In the context of cyber space, activities such as hacking private

[13] Al-Ghazali, Abu Hamid Muhammad ibn Muhammad. Ihya' 'Ulum al-Din. Cairo: Dar al-Hadith, 1999, Vol. 2, p. 92.

[14] The Qur'an. Surah Al-Hujurat 49:12. Cairo: Dar al-Mushaf al-Sharif, n.d.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

accounts, unauthorized surveillance, and leaking confidential data fall directly under this prohibition. The concept of Satr ensures that individuals' dignity and privacy are protected, making digital privacy violations a serious ethical and legal breach in Islamic law.

Application of Ta'zir Punishments in Cyber Crimes

Ta'zir refers to discretionary punishments in Islamic criminal law that are applied to offenses for which no fixed penalty (Hudud) or retaliation (Qisas) is prescribed. Cyber crimes largely fall under the category of Ta'zir because they are modern offenses that were not explicitly defined in classical jurisprudence. Judges and legal authorities are therefore empowered to determine appropriate punishments based on the severity, harm, and social impact of the offense.

Cyber crimes such as hacking, digital fraud, identity theft, cyber harassment, and data breaches can be effectively addressed through Ta'zir penalties, which may include fines, imprisonment, digital restrictions, or rehabilitation measures. The flexibility of Ta'zir allows Islamic law to adapt to evolving technological challenges while maintaining its ethical foundation.Imam Ibn Taymiyyah states:

"التعزير يكون بحسب المصلحة ودفع الضرر[15]".

"Discretionary punishment is determined according to public interest and the prevention of harm."

Ibn Taymiyyah emphasizes the flexible nature of Ta'zir, which is based on achieving public welfare and preventing harm. In cyber crime cases, this principle allows legal authorities to impose appropriate penalties depending on the nature and impact of the offense. For example, large-scale cyber fraud may require stricter penalties than minor privacy violations. This adaptability ensures that Islamic criminal law remains relevant in addressing modern cyber threats while upholding justice and societal protection.

Financial crimes, privacy violations, and discretionary punishments demonstrate the adaptability of Islamic criminal law in addressing contemporary cyber challenges. The principles of Hifz al-Mal, Satr, and Ta'zir provide a comprehensive ethical and legal framework for regulating digital offenses. Together, these principles ensure that Islamic law remains capable of responding effectively to modern cyber crimes while preserving justice, dignity, and social order in the digital age.

Comparative Analysis of Islamic and International Law

Foundations of Criminal Responsibility

Criminal responsibility is a fundamental concept in both Islamic criminal law and modern international legal systems, though its philosophical foundations and scope differ significantly. In international law, criminal responsibility is primarily based on the principle of mens rea (criminal intent) and actus reus (criminal act), requiring proof of intent, action, and causation. Modern legal systems emphasize individual accountability, procedural safeguards, and evidentiary standards to determine guilt.

In Islamic criminal law, criminal responsibility (al-mas'uliyyah al-jina'iyyah) is grounded in moral accountability before God and legal accountability before society. It is based on the capacity (ahliyyah) of the individual, including maturity, sanity, and free will. Islamic jurisprudence integrates both intention (niyyah) and action, while also emphasizing ethical and spiritual dimensions of accountability. In cyber crimes, both systems face the challenge of determining

[15] Ibn Taymiyyah, Ahmad ibn Abd al-Halim. Majmu' al-Fatawa. Riyadh: King Fahd Complex, 1995, Vol. 28, p. 146.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

intent in digital environments where anonymity and technological mediation complicate evidence and attribution.Imam Al-Ghazali states:

"الأحكام تدور مع المقاصد وجودًا وعدمًا[16]".

"Legal rulings revolve around intentions; they exist or cease based on intentions."

Al-Ghazali's principle highlights the centrality of intention in determining legal and moral responsibility. In cyber crime cases, establishing intent is often complex due to anonymity and digital masking techniques. However, both Islamic and modern legal systems recognize that liability cannot be established without demonstrating intent or negligence. This convergence shows that despite methodological differences, both systems acknowledge the importance of mental state in assigning criminal responsibility.

Concept of Justice: Shariah vs Modern Legal Systems

The concept of justice ('adl) occupies a central position in both Shariah and modern legal systems, yet its philosophical foundations and applications differ significantly. In Islamic law, justice is rooted in divine revelation and is considered an absolute moral obligation that transcends human interpretation. It is not merely a procedural mechanism but a comprehensive ethical framework aimed at achieving balance, fairness, and protection of human dignity in both worldly and spiritual dimensions.

In contrast, modern legal systems define justice primarily in procedural and institutional terms, emphasizing equality before the law, due process, and the protection of individual rights within a codified legal structure. While Islamic law integrates morality and spirituality into justice, modern systems focus more on legal positivism and institutional enforcement. Despite these differences, both frameworks aim to ensure fairness, prevent oppression, and maintain social order, especially in complex domains such as cyber law and digital governance.

Imam Ibn Taymiyyah states:

"إن الله يقيم الدولة العادلة وإن كانت كافرة، ولا يقيم الظالمة وإن كانت مسلمة[17]".

"Indeed, Allah supports a just state even if it is non-believing, and He does not support an unjust state even if it is Muslim."

Ibn Taymiyyah's statement underscores the universal importance of justice as a governing principle. In comparison with modern legal systems, this highlights that justice is not limited to religious or cultural boundaries but is a universal value essential for governance. In cyber law, where global cooperation is necessary, this principle becomes particularly relevant, as fairness and justice must be maintained across different legal traditions and jurisdictions.

Digital Evidence and Forensic Systems

Digital evidence has become a critical component of modern legal proceedings, especially in cases involving cyber crimes. It includes electronic data such as emails, server logs, IP addresses, digital communications, multimedia files, and metadata extracted from devices and networks. Modern forensic systems rely on advanced technologies such as data recovery tools,

[16] Al-Ghazali, Abu Hamid Muhammad ibn Muhammad. Ihya' 'Ulum al-Din. Cairo: Dar al-Hadith, 1999, Vol. 1, p. 65.

[17] Ibn Taymiyyah, Ahmad ibn Abd al-Halim. Majmu' al-Fatawa. Riyadh: King Fahd Complex, 1995, Vol. 28, p. 146.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

network analysis, artificial intelligence, and blockchain verification to ensure the integrity and authenticity of digital evidence.

In international law, strict protocols govern the collection, preservation, and presentation of electronic evidence to ensure admissibility in court. Issues such as data integrity, chain of custody, and authenticity verification are central to forensic procedures. Similarly, Islamic legal principles also emphasize strong evidentiary standards, requiring certainty (yaqeen) and the avoidance of doubt (shubha) in judicial decisions.

Imam Al-Shatibi states:

"اليقين لا يزول بالشك، والأحكام تبنى على الأدلة القطعية[18]".

"Certainty is not removed by doubt, and rulings are based on definitive evidence."

Al-Shatibi's principle aligns closely with modern forensic standards that require reliable and verifiable digital evidence for conviction. In cyber crime cases, where data can be manipulated or falsified, ensuring authenticity is crucial. Both Islamic and modern legal systems emphasize that judgments cannot be based on uncertainty or incomplete information. Therefore, digital forensic systems serve as a modern extension of the Islamic principle of certainty in judicial decision-making.

The comparative analysis of criminal responsibility, justice, and digital evidence demonstrates significant areas of convergence between Islamic and modern legal systems. While their philosophical foundations differ, both systems emphasize accountability, fairness, and evidentiary certainty. In the context of cyber crimes, these shared principles provide a strong basis for developing integrated legal responses that combine ethical depth with technological precision, ensuring justice in both traditional and digital domains.

Punishment Systems: Hudood, Ta'zir vs Penal Codes

Punishment systems in Islamic law and modern international legal systems differ in structure, philosophy, and application, yet both aim to establish justice and deter criminal behavior. In Islamic criminal law, punishments are primarily categorized into Hudood (fixed punishments prescribed by divine texts), Qisas (retaliation-based justice), and Ta'zir (discretionary punishments determined by judicial authority). Hudood offenses such as theft, adultery, and highway robbery have fixed penalties, while Ta'zir covers a broad range of offenses, including modern crimes like cyber fraud and digital harassment. In contrast, modern penal codes are human-made legal systems that define crimes and assign punishments through legislative processes. These systems emphasize proportionality, rehabilitation, deterrence, and social reintegration. Unlike Islamic law, modern penal systems are flexible and continuously evolving through statutory reforms and judicial interpretation. Despite structural differences, both systems share the objective of protecting society, ensuring justice, and preventing harm.

Imam Ibn Qayyim al-Jawziyyah states:

"الشريعة مبناها على العدل والرحمة، وكل حكم خرج عن العدل فهو ليس من الشريعة[19]".

[18] Al-Shatibi, Ibrahim ibn Musa. Al-Muwafaqat fi Usul al-Shari'ah. Beirut: Dar al-Kutub al-'Ilmiyyah, 2003, Vol. 2, p. 92.

[19] Ibn Qayyim al-Jawziyyah, Muhammad ibn Abi Bakr. I'lam al-Muwaqqi'in 'an Rabb al-'Alamin. Beirut: Dar al-Kutub al-'Ilmiyyah, 1991, Vol. 3, p. 11.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

"Shariah is founded upon justice and mercy, and any ruling that departs from justice is not part of Shariah."

Ibn Qayyim's principle highlights that the essence of Islamic punishment is rooted in justice and mercy rather than rigid enforcement. This aligns in some ways with modern penal philosophies that emphasize fairness, proportionality, and rehabilitation. In cyber crime contexts, where offenses vary widely in severity, the flexibility of Ta'zir allows Islamic law to adapt punishments appropriately. Similarly, modern penal codes use discretionary sentencing to address complex digital offenses, showing a functional convergence between the two systems.

Rights and Legal Protection of Victims

Victim protection has become a central concern in both Islamic criminal law and modern international legal systems. In contemporary legal frameworks, victims' rights include access to justice, fair trial guarantees, compensation, psychological support, and protection from further harm. Cyber crimes such as identity theft, online harassment, financial fraud, and data breaches have significantly increased the need for robust victim protection mechanisms in the digital age.Islamic law also places strong emphasis on the rights of victims, particularly through the principles of restitution (diyah), compensation, and the removal of harm (raf' al-darar). It ensures that victims are not only recognized legally but also morally protected, with strong emphasis on restoring justice and repairing harm caused by the offender.

Imam Al-Ghazali states:

"رفع الضرر واجب في الشرع، ولا يجوز الإضرار بالناس بأي حال[20]".

"Removing harm is obligatory in Shariah, and it is not permissible to harm people under any circumstance."

Al-Ghazali's principle forms the ethical foundation for victim protection in Islamic law. In the context of cyber crimes, this principle directly applies to cases involving online defamation, financial exploitation, and privacy violations. Both Islamic and modern legal systems recognize that victims must be protected from harm and provided with remedies. While modern law focuses on legal compensation and institutional support, Islamic law integrates moral responsibility with legal restitution, ensuring comprehensive victim protection.

The comparison between Hudood, Ta'zir, and modern penal codes reveals both structural differences and functional similarities in punishment systems. While Islamic law emphasizes divine authority and moral accountability, modern systems prioritize legislative flexibility and procedural justice. Similarly, both traditions strongly emphasize the protection of victims and the restoration of harm. In the context of cyber crimes, these shared objectives highlight the potential for integrating ethical and legal frameworks to ensure justice, deterrence, and comprehensive victim protection in both physical and digital environments.

Contemporary Challenges and Islamic Legal Reforms

Cyber Fraud, Hacking, and Identity Crimes

Cyber fraud, hacking, and identity-related crimes represent some of the most serious challenges in the contemporary digital landscape. These offenses include unauthorized access to computer systems, financial fraud through phishing or digital manipulation, identity theft, and the misuse of personal data for unlawful gain. With the increasing dependence on digital platforms for

[20] Al-Ghazali, Abu Hamid Muhammad ibn Muhammad. Ihya' 'Ulum al-Din. Cairo: Dar al-Hadith, 1999, Vol. 2, p. 95.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

banking, communication, and governance, such crimes have acquired global significance and pose severe threats to individual security, economic stability, and institutional trust.

From an Islamic legal perspective, these crimes fall directly under the violation of Hifz al-Mal (protection of wealth) and Hifz al-Nafs (protection of life and security), as they lead to financial loss, psychological harm, and social disruption. The concept of Ta'zir provides a flexible framework for addressing such emerging offenses, allowing judicial authorities to impose appropriate punishments based on the severity and impact of the crime.Imam Ibn Taymiyyah states:

"أخذ أموال الناس بغير حق من أعظم أنواع الفساد في الأرض[21]".

"Taking people's wealth without right is one of the greatest forms of corruption on earth."

Ibn Taymiyyah's statement clearly reflects the ethical and legal prohibition of financial injustice. Cyber fraud and identity theft represent modern technological forms of the same wrongdoing, where wealth is unlawfully acquired through deception or digital manipulation. Islamic law treats such actions as serious violations of public and private rights, requiring strict legal accountability. The flexibility of Islamic criminal law allows these crimes to be addressed under Ta'zir, ensuring justice is maintained in evolving technological contexts.

Social Media Crimes and Defamation

Social media platforms have transformed communication but have also given rise to new forms of criminal behavior, including defamation, cyberbullying, spreading false information, character assassination, and the unauthorized sharing of private content. These offenses have serious consequences for individuals' reputations, mental health, and social standing. In many cases, digital defamation spreads rapidly and becomes irreversible, amplifying harm far beyond traditional forms of slander.

Islamic law places strong emphasis on the protection of honour (Hifz al-'Ird) and strictly prohibits backbiting (ghibah), slander (buhtan), and spreading false accusations. Social media crimes therefore fall directly within the scope of moral and legal prohibition in Shariah, requiring accountability and restitution for harm caused.The Qur'an states:

"وَيْلٌ لِكُلِّ هُمَزَةٍ لُمَزَةٍ"

"Woe to every slanderer and backbiter."

This Qur'anic verse highlights the severe moral condemnation of defamation and character assassination. In the digital age, social media platforms often amplify such harmful behavior, making defamation widespread and instantaneous. Islamic teachings emphasize that protecting human dignity is essential, and any form of public humiliation or false accusation is a serious ethical violation. Therefore, social media crimes are not merely technological issues but profound moral transgressions requiring legal and ethical reform.

Cyber fraud, hackin[22]g, identity theft, and social media defamation represent evolving challenges that demand both legal and ethical responses. Islamic criminal law, through principles such as Hifz al-Mal, Hifz al-'Ird, and Ta'zir, provides a flexible and comprehensive framework for addressing these issues. At the same time, contemporary legal reforms are necessary to adapt to

[21] Ibn Taymiyyah, Ahmad ibn Abd al-Halim. Majmu' al-Fatawa. Riyadh: King Fahd Complex, 1995, Vol. 29, p. 123.

[22] The Qur'an. Surah Al-Humazah 104:1. Cairo: Dar al-Mushaf al-Sharif, n.d.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

technological advancements. The integration of Islamic ethical principles with modern regulatory mechanisms ensures effective protection of individuals, preservation of trust, and maintenance of social order in the digital era.

Artificial Intelligence and Automated Cyber Crimes

Artificial Intelligence (AI) has introduced a new dimension to cyber security and cyber crime. While AI systems are widely used for automation, prediction, and digital optimization, they are also increasingly exploited for criminal purposes. Automated cyber crimes include AI-driven hacking, deepfake technology, algorithmic fraud, automated phishing attacks, bot-based identity theft, and large-scale data manipulation. These crimes are particularly dangerous because they operate at high speed, require minimal human intervention, and can target millions of users simultaneously.

From a legal and ethical perspective, AI-generated cyber crimes raise complex questions about accountability, intent, and responsibility. Islamic criminal law, which emphasizes moral intention (niyyah) and human agency, provides a foundational framework for addressing such issues through the principle of Ta'zir, allowing authorities to assign liability based on harm and causation even in technologically complex scenarios.Imam Al-Shatibi states:

"الأحكام تدور مع عللها وجوداً وعدما[23]".

"Legal rulings revolve around their underlying causes, existing when causes exist and disappearing when they do not."

Al-Shatibi's principle is highly relevant to AI-driven cyber crimes, where traditional notions of direct human intent may be blurred. In automated systems, harm can occur through programmed algorithms rather than direct human action. This principle allows Islamic legal reasoning to focus on the cause and effect of harm rather than solely on direct human intervention. Thus, if AI systems are used to commit fraud or digital attacks, responsibility is established based on causation and control, ensuring accountability even in advanced technological environments.

Digital Surveillance and Ethical Issues

Digital surveillance has become an essential yet controversial aspect of modern governance and cybersecurity. Governments, corporations, and institutions increasingly rely on surveillance technologies such as facial recognition, data tracking, metadata analysis, and online monitoring to ensure security and prevent cyber threats. However, excessive surveillance raises serious ethical concerns related to privacy invasion, misuse of personal data, and potential abuse of power.

In Islamic ethical and legal tradition, privacy (Satr) and protection of personal dignity are fundamental principles. Surveillance without legitimate justification contradicts the moral injunction against spying and violating private spaces. Therefore, Islamic law requires a balance between public security and individual privacy, ensuring that surveillance is conducted only within ethical and legal boundaries.The Qur'an states:

"وَلَا تَجَسَّسُوا[24]"

"And do not spy on one another."

This Qur'anic directive establishes a clear prohibition against unwarranted surveillance and intrusion into private lives. In the digital age, surveillance technologies can easily violate this principle if used without ethical constraints. While security monitoring is necessary to prevent

[23] Al-Shatibi, Ibrahim ibn Musa. Al-Muwafaqat fi Usul al-Shari'ah. Beirut: Dar al-Kutub al-'Ilmiyyah, 2003, Vol. 2, p. 180.

[24] The Qur'an. Surah Al-Hujurat 49:12. Cairo: Dar al-Mushaf al-Sharif, n.d.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.04 No.01 (2026)

cyber threats, Islamic teachings require that such measures be justified, proportionate, and free from abuse. This balance ensures that public safety does not come at the cost of individual dignity and privacy.

Need for a Modern Islamic Cyber Law Framework

The rapid expansion of digital technologies has created unprecedented legal challenges that require a comprehensive and adaptive legal response. Existing classical Islamic legal frameworks, while rich in ethical and jurisprudential principles, need structured modernization to effectively address contemporary cyber realities such as AI crimes, data protection, digital fraud, and cross-border cyber offenses.

A modern Islamic cyber law framework would integrate foundational principles of Shariah such as justice (‘adl), prevention of harm (darar), protection of wealth (Hifz al-Mal), and protection of dignity (Hifz al-‘Ird)—with contemporary legal instruments, technological expertise, and international cooperation standards. Such a framework would allow Islamic legal systems to remain relevant and effective in regulating modern digital environments.

Imam Ibn Qayyim al-Jawziyyah states:

"الشريعة مبناها على مصالح العباد في المعاش والمعاد[25]".

"Shariah is based upon the welfare of human beings in both this life and the hereafter."

Ibn Qayyim’s statement highlights the objective-based nature of Islamic law, emphasizing human welfare as its central aim. A modern Islamic cyber law framework must therefore prioritize public interest, digital security, and ethical governance. By integrating classical principles with modern legal tools, Islamic law can effectively address cyber crime while preserving its moral and philosophical foundations. This ensures that Shariah remains adaptable, dynamic, and relevant in the digital age.

Artificial intelligence, digital surveillance, and the evolving nature of cyber crime present significant challenges for both modern and Islamic legal systems. While technological advancement increases complexity, Islamic jurisprudence provides adaptable principles that can address emerging issues through Ta’zir, ethical regulation, and maqasid-based reasoning. A modern Islamic cyber law framework that integrates traditional values with contemporary legal and technological tools is essential for ensuring justice, security, and ethical governance in the digital era.

Bibliography

1. Al-Ghazali, Abu Hamid Muhammad ibn Muhammad. Al-Mustasfa min ‘Ilm al-Usul. Beirut: Dar al-Kutub al-‘Ilmiyyah, 1993.
2. Al-Ghazali, Abu Hamid Muhammad ibn Muhammad. Ihya’ ‘Ulum al-Din. Cairo: Dar al-Hadith, 1999.
3. Al-Mawardi, Abu al-Hasan Ali ibn Muhammad. Al-Ahkam al-Sultaniyyah. Cairo: Dar al-Hadith, 2001.
4. Al-Shatibi, Ibrahim ibn Musa. Al-Muwafaqat fi Usul al-Shari‘ah. Beirut: Dar al-Kutub al-‘Ilmiyyah, 2003.

[25] Ibn Qayyim al-Jawziyyah, Muhammad ibn Abi Bakr. I‘lam al-Muwaqqi‘in ‘an Rabb al-‘Alamin. Beirut: Dar al-Kutub al-‘Ilmiyyah, 1991, Vol. 3, p. 14.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR

5. Ibn Khaldun, ‘Abd al-Rahman ibn Muhammad. Al-Muqaddimah. Beirut: Dar al-Fikr, 2004.
6. Ibn Qayyim al-Jawziyyah, Muhammad ibn Abi Bakr. I‘lam al-Muwaqqi‘in ‘an Rabb al-‘Alamin. Beirut: Dar al-Kutub al-‘Ilmiyyah, 1991.
7. Ibn Taymiyyah, Ahmad ibn Abd al-Halim. Majmu‘ al-Fatawa. Riyadh: King Fahd Complex for the Printing of the Holy Qur’an, 1995.
8. Ibn Taymiyyah, Ahmad ibn Abd al-Halim. Al-Siyasah al-Shar‘iyyah fi Islah al-Ra‘i wa al-Ra‘iyyah. Riyadh: King Fahd Complex for the Printing of the Holy Qur’an, 1998.
9. Al-Shawkani, Muhammad ibn Ali. Nayl al-Awtar. Beirut: Dar al-Fikr, 2002.
10. Al-Azami, Muhammad Mustafa. Studies in Early Hadith Literature. Indianapolis: American Trust Publications, 1978.
11. Hassan, Husayn Hamid. The Evaluation of Hadith Literature: Historical and Methodological Approaches. Karachi: Islamic Research Academy, 1992.
12. Council of Europe. Convention on Cybercrime (Budapest Convention). Strasbourg: Council of Europe Treaty Series, 2001.
13. United Nations. Reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. New York: United Nations, 2015.
14. European Union. General Data Protection Regulation (GDPR). Brussels: European Union Publications, 2016.
15. Brenner, Susan W. Cybercrime and the Law: Challenges and Solutions. New York: Norton Law Publications, 2010.
16. Wall, David S. Cybercrime: The Transformation of Crime in the Information Age. Cambridge: Polity Press, 2007.