ORIGINAL ARTICLE

International Journal of Social Sciences and Business Research

Islamic Law and Cybercrime: Developing a Shariah-Based Framework for Digital Security in Pakistan

Muhammad Awais

1 **Muhammad Awais**	**Contribution** Department of Management Sciences, Abasyn University Peshawar
Correspondence author Muhammad Awais Department of Management Sciences, Abasyn University Peshawar owaiskhan523@gmail.com	Submitted for Publication 05-09-2026 Revision Received 09-09-2026 Accepted for Publication 27-09-2026

ABSTRACT

The development of digital technologies has had an impact on almost every area of life in the country, including communications, trade, education, finance, and government administration, etc. However, in addition to the benefits offered by these innovations, criminal activities such as hacking, fraud, online stalking, illegal access, identity theft, data theft, defamation, and harassment have become a threat not only to individuals but also to businesses. In Pakistan such offences are governed by the Prevention of Electronic Crimes Act (PECA) of 2016 and the National Cyber Security Policy of 2021. Nevertheless, the law is still developing through the introduction of amendments and new regulations. Moreover, Islamic law provides another method of addressing cybercrime control since the principles of Islam such as ʿadl (justice), amānah (trust), protection from harm (ḍarar), protection of privacy, protection of property, and maṣlaḥah (the public good) are relevant. Therefore, the purpose of this paper is to propose a Shariah-based solution to the problem of cybersecurity in Pakistan on the basis of the principles of maqāṣid al-sharīʿah and taʿzīr. The paper states that cybercrimes are not ḥudūd offences, which means that they should be dealt with by means of taʿzīr.

Keywords: Islamic laws, cybercrime, Sharia, cyber security, maqasid al shariah, ta'zir

This is an open access article distributed under the terms of the Attribution Creative Commons-Noncommercial (CC BY-by 4.0) (https://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

INTRODUCTION

Information and communication technologies have led to major changes in a wide range of areas of life in Pakistan. The widespread use of technologies such as smartphones, social media, Internet banking, e-commerce, cloud computing, and artificial intelligence has made communication, economic growth, and the acquisition of information much easier. At the same time, the country's security situation has become more dangerous since cybercrime has increased in Pakistan. A number of cyber threats are encountered by individuals, companies, universities, banks, governmental organisations, and the country's infrastructure as a result of hacking, identity theft, phishing, and financial fraud. For this reason, the problem of cybersecurity has become extremely important. Cybercrimes have certain features that set them apart from other types of crime, such as remoteness, anonymity, speed, and international reach. A single cybercriminal is capable of affecting hundreds or even thousands of people, and as a result there are likely to be financial losses, breaches of privacy, damage to reputation, psychological trauma, disruptions to business operations, and a threat to national security. Since internet banking has been introduced in Pakistan, it has been necessary to secure both the transactions and personal data. In a similar way, the introduction of social networking sites has given cybercriminals the opportunity to engage in cyberbullying, identity theft, defamation, the spread of false information, and the illegal posting of personal data. It therefore follows that conventional methods of handling crime are no longer suitable in this situation.

In order to deal with the problems referred to, Pakistan has drawn up laws and policies. Firstly, the Prevention of Electronic Crimes Act (PECA) was passed in 2016, the aim of which is to establish the legal provisions for various offences connected with information systems and electronic communication, such as illegal access to information systems, interference with information systems, electronic fraud, identity-related offences, and certain aspects of cyberbullying. The Prevention of Electronic Crimes Act is a crucial legal tool when it comes to investigation, prosecution and international cooperation. regarding electronic crimes (Government of Pakistan, 2016). Moreover, the National Cyber Security Policy 2021 seeks to create a secure, sustainable, and trusted cyberspace by capacity building, cybersecurity standards development, cooperation, awareness raising, and protection of the national digital infrastructure (Government of Pakistan, 2021). However, taking into account the emergence of novel technologies and threats, it is necessary to develop a strategy of a more complex nature that would not be focused solely on punishment. The Law of Islam is one of the most effective normative perspectives that could help solve these issues. Although traditional Islamic jurisprudence has been elaborated long ago before the computer and internet era, it still encompasses a principle that is quite wide in its scope and allows dealing with new forms of behaviors through methods like qiyās (analogy), maṣlaḥah (interest), sadd al-dharā'iʿ (prevention of means of committing harm), and ijtihād (independent reasoning). Thus, these new forms of cyber crimes can be assessed depending

on the form of the behavior and its outcomes rather than the technology itself. For instance, an unauthorized access to other people's computer systems under the prohibition of all acts of infringement and spying as well as stealing someone else's money should be seen as a prohibition of certain actions regarded as an infringement upon the property of others according to Islam (Qur'an 2:188). The maqāṣid al-sharīʿah can become an excellent platform for creating a security strategy based on the law of Islam. The main goal of the Islamic law is to guarantee that basic human values are observed in the community. They include religion, life, intellect, lineage, and property (al-Ghazālī, 1997; al-Shāṭibī, 1997). At the time of the technology and digitalization era, these objectives of the law can be supplemented by personal information, digital property, organizational information, online identity, and integrity of digital technologies. Lā ḍarar wa lā ḍirār has a special significance for cyber crimes as there is no doubt that they have adverse impacts on individuals, organizations, and communities (Ibn Mājah, 2007). Another crucial principle of Islamic law is taʿzīr, which is used to define the adequate punishment of acts that have no specific amount of punishment (ḥudūd). Majority of the modern crimes associated with the cybercrime cannot fit into ḥudūd crimes; therefore, it is necessary to use the taʿzīr principle to punish the offender according to the degree of the crime and its influence on the public interest. The contemporary scientific literature touches upon the problem of the role of the Islamic legal principles in cybercrime (Bilal & Khan, 2022; Abrar, 2026). Thus, the primary goal of the present research is the development of the concept of digital security in terms of Islamic perspective in Pakistan, which involves combining Islamic principles of law with the existing legislation on cybercrimes and cyber security in the country. Islamic law can be a solid ground for the positive law in terms of attaining the mentioned goals.

2. Concept of Cybercrime from the Islamic Point of View

Cybercrime can be defined as the crime committed with the help of the computer, information systems, franchises, and/or any equipment in the process of committing the crime. These types of crimes include: illegal access to computer; information stealing; identity theft; financial crime; cyber stalking; interference with computer system; web harassment; rumor mongering. From the Islamic point of view, it is important to judge the legality of any act according to its consequences and not only to the way of performing of the particular act. There is no ethical value that a computer, cell phone, website or any other kind of artificial intelligence device can have since the latter depends on what is done through the former. According to the Qur'an, there are strict regulations concerning the respect of privacy:

"Do not spy on one another." (Qur'an 49:12).

It is especially relevant for the unauthorized access to people's accounts, eavesdropping on conversations, unlawful surveillance, and stealing of personal information. Furthermore, Islam forbids to possess something that does not belong to a person without any valid reason: "Do not devour one another's property wrongfully." (Qur'an 2:188). It is applicable to online banking scams, cryptocurrency scams, phishing, etc. Privacy and good communication are highly respected in Islam. The Qur'an tells Muslims to make sure that the information is correct (Qur'an 49:6).

3. Maqāṣid al-Sharīʿah and Digital Security

Maqāṣid al-sharīʿah possess all the necessary theoretical background for the development of Islamic approaches to combating cyber crimes. The classical approach of Islamic law defines the preservation of religion (ḥifẓ al-dīn), life (ḥifẓ al-nafs), intellect (ḥifẓ al-ʿaql), family (ḥifẓ al-nasl), and property (ḥifẓ al-māl) as the main aims of Shariah (al-Ghazālī, 1997; al-Shāṭibī, 1997). These objectives can be used in relation to cyberspace as well. Let us discuss this point in more detail. First of all, the protection of property implies the protection from online fraud, unauthorized transactions, ransomware, stealing valuable items online, and protection from intellectual property rights infringement. The protection of intellect implies protection from technologies that mislead people with the help of fraudulent information and malware.

The protection of honor and family implies protection from cyber stalking, sexual abuse, illegal sharing of personal data, and cyberbullying. The protection of life becomes vital when cyber criminals attack such vital services as hospitals, ambulances, critical infrastructures and technologies that fail to work may harm physical well-being.

4. The Principle of La Ḍarar and Cybercrime

The first of the rules of Islamic law related to cyber crime is the following one "Lā ḍarar wa lā ḍirār" and it means "No harm shall be inflicted, nor should harm be reciprocated." This rule comes from prophetic hadith and it means that no harm can be done to other person in general (Ibn Mājah, 2007). The rule can be applied in the Internet rather broadly, since the hacking of other accounts, the theft of the personal data, the damage of the electronic data, the installation of the malware, the commission of the cyber crime, and the defamation of other individual can be considered the harm per se. Moreover, this principle can be used for the crimes committed in cyberspace which do not belong to any traditional crime category in criminal law. As the experts of the Islamic law state nowadays, this principle can be considered as the basis for all crimes committed in the modern technological environment from the legal point of view (Al-Anazi, 2026).

5. Cybercrime and the Islamic Concept of Taʿzīr

These three classifications of offenses and punishments in the classical theory of Islamic law are ḥudūd, qiṣāṣ/diyāt, and taʿzīr. There are many justifications for addressing cybercrime through amending the taʿzīr as most of the cybercrimes were not related to any ḥadd as there was no specific punishment for hacking, phishing, identity theft, and many more criminal activities.

Taʿzīr means that the nation or court will have the right to impose punishment on the offender for any crime as there is no specified punishment for that offense. In this way, taʿzīr aims to both punish and deter offenders. Moreover, the aim of taʿzīr is also to deter offenders from committing the crime again and ensure the safety of the offenders. Additionally, researchers support this approach because the principle of taʿzīr is the basis for many types of cybercrimes (Abrar, 2026).

However, taʿzīr should be applied through the reasonable use of evidence.

6. **Proposed Shariah-Based Framework for Pakistan**

The Shariah-based framework for digital security in Pakistan may consist of seven principles:

Principle	Islamic foundation	Digital application
Privacy	Qur'an 49:12	Protection against unauthorized access and surveillance
Property	Qur'an 2:188	Prevention of online fraud, theft and financial crimes
Truthfulness	Qur'an 33:70; 49:6	Combating misinformation and fabricated digital content
Prevention of harm	*Lā ḍarar wa lā ḍirār*	Prevention of hacking, malware and cyber harassment
Trust	*Amānah*	Responsible handling of personal and institutional data
Justice	*ʿAdl*	Fair investigation, trial and proportionate punishment
Public interest	*Maṣlaḥah*	Protection of critical infrastructure and national digital systems

6.1 Prevention

First of all, the first characteristic of any Shariah system of dealing with cybercrimes in Pakistan is prevention. Indeed, in the Islamic tradition, there are several issues that should be taken care of for the sake of not inflicting any kind of injury or harm to oneself or others. According to the rule lā ḍarar wa lā ḍirār (neither to inflict harm nor be harmed), all actions that may potentially cause injuries should be prevented (Ibn Mājah, 2007). When those actions take place in cyberspace, it means that people, companies, and government have to do their best in order to prevent the emergence of different crimes in cyberspace, including hacking, identity theft, cyberstalking, data theft, viruses, etc.

It is extremely important to make people familiar with such issues as cybersecurity and digital ethics in school, in work places, in governmental bodies, and in the society in general. People should be aware of such terms as password security, phishing, privacy, social media, and consequences of illegal entering into computer systems and networks. That knowledge goes along with the concept of amānah that is the responsibility of a person to manage information and resources. Indeed, according to the Qur'an, believers should return amānah to its owner (Qur'an 4:58).

Along with creating regulatory bodies, the measures aimed at prevention include the use of both technologies and institutions. The major players, such as governmental organizations, banks, universities, hospitals, and private firms, have to develop measures in order to prevent cyber attacks. In this respect, it is necessary to mention the National Cyber Security Policy 2021 of Pakistan. Moreover, there is a possibility to use the Muslim method of verification of information as an extremely useful source which could protect people from manipulations online. As it is mentioned in one of the verses of the Quran, it is required to verify information prior to using it. Thus, verification of digital information will prevent misinformation and damage to reputation. In conclusion, all necessary preventive measures could be taken only with active collaboration of legislative authorities and IT specialists, Islamic scholars and educators. It will guarantee the efficiency of cybersecurity as well as compliance with the traditional Islamic principles of justice, honesty and security from any harm.

6.2 Privacy and Data Protection

Privacy and data protection are crucial parts of the digital security framework, and the elements of Islamic law are able to facilitate them as well. Indeed, what needs to be emphasized is that there is a prohibition to intrude into someone's privacy without his/her permission as stated in the Qur'an as "Do not spy on one another" (Qur'an 49:12). In this respect, it is possible to underline that the mentioned norm is rather valuable considering the current reality when it is possible to obtain all types of information about a person (including private information, photos, financial issues, passwords, communications, and so on), and this person him/herself can not even notice it. Thus, it is possible to note that access to someone's e-mail address, social media accounts, mobile phone, database, cloud, etc., without having the right to do it violates the principle of privacy in the context of the Islamic religion. The issue of amānah (trust) is crucial in terms of the Islamic law. It means that both individuals and groups have to ensure the safety of information that was given to them as the trust. The sacred book of Muslims, the Qur'an, teaches the followers to return the trust to the legitimate owner of the information. Considering the context of the digital communication, the organizations that obtained personal information of the clients have to perceive it as trust, but not the resource that can be used freely. Having obtained this information, the organization should not gather unnecessary information and provide restricted access to it. Lā ḍarar wa lā ḍirār is another concept that proves the importance of data protection as any violation of the data security leads to various types of losses (including financial, psychological, social, and reputational ones; Ibn Mājah, 2007). As in the case of the presence of the cybersecurity strategy for Pakistan that ensures the security of information systems (Government of Pakistan, 2021). It needs to be stated that in order to create the system of data protection that is based on the Shariah, some principles need to be taken into consideration. They include informed consent, confidentiality, secure storage, limited access, breach notifications, and accountability. The combination of the Islamic tradition and modern data protection will create the feeling of security among the citizens of Pakistan (Bilal & Khan, 2022).

6.3 Digital Evidence

It goes without saying that digital evidence is of utmost importance when it comes to investigation of cybercrimes, because cybercrimes inevitably leave traces that can be detected

on computers, on mobile devices, servers, databases, cloud computing, communications networks, etc. Therefore, a digital security policy for Pakistan which should be formed in accordance with the Shariah law should contain certain specific rules regarding collection, protection, authentication, verification, and presentation of digital evidence. The entire approach should contain a necessary background that should be provided based on the principle of verification that is stated in the Quran: "...the believers should not accept anything unless they investigate it..." (Qur'an 49:6). It means that any accusations cannot be made unless any grounds are found for them in the form of digital evidence. Nevertheless, the Islamic law pays much attention to the reliability of evidence and justice. Evidence has to be examined in an objective manner and prove to be sufficiently reliable. In other words, if any cybercrime took place, it implies that electronic records have to be properly secured, and there must be an established chain of custody of the evidence from the moment of collection to presentation in court. There is a concept of ʿadl (justice) in Islam which presupposes that cognitive evidence must be examined objectively, and digital evidence cannot be considered as evidence simply because of its digital nature. It is important for the experts to examine the information and find out if the information was manipulated, tampered with, modified, and if the information was produced using the wrong methods. Due to the rapid development of artificial intelligence and editing software, it is becoming extremely important. The Prevention of Electronic Crimes Act of Pakistan forms the basis of investigation of electronic crimes in Pakistan. The act provides the Islamic approach to obtaining authentication, credibility, objectivity, and justice. Accordingly, digital evidence must not only be authentic but also truthful in accordance with the Islamic law.

6.4 Proportionate Punishment

The principle of proportionate punishment is also one of the main elements of Sharia-based policy targeted at cybercrime prevention in Pakistan. There is no need for the provision of equal punishment for all criminal acts in the Islamic legal system. On the contrary, the following aspects can be taken into account while considering the reaction to the criminals' deeds: the nature of crime, the severity of crime, intentionality of the criminal act, circumstances of the crime, etc., in addition to the other interests of society as a whole. “Stand firmly for justice” (Qur'an 4:135) is clearly indicated in the Qur'an. The vast majority of most modern cybercrimes cannot be considered as ḥudūd crimes with pre-assigned punishments. In such a way, most modern cybercrimes should be considered as taʿzīr crimes because they allow punishing offenders with certain punishments but do not provide specific punishments (Kamali, 2008). The main principle of taʿzīr can be used in the field of cybercrimes as they can be characterized by high diversity with regard to crime severity. For example, in one case, the illegal access to a system can cause no damages; in another case, there may be considerable damages. This issue is related to online bullying, identity theft, financial fraud, ransomware attacks, and many others. With regard to punishment, there are several issues that should be considered in order to provide the appropriate punishment including intentions of the offender with regard to the crime, damages done to others, the number of victims, severity of the crime, and many others. Depending on the case, it may include warning, penalty, or even some educational measures. However, in the case of serious crimes, more severe punishment should be used. The compensation for the victims can be considered as highly relevant to the principle of asset protection and harm preventiveness that is one of the main principles of the Islamic law (Ibn Mājah, 2007).

The Prevention of Electronic Crimes Act of Pakistan is an act that allows defining the types of electronic offenses (Government of Pakistan, 2016). The Shariah approach should be used in order to establish the legal framework, and arbitrariness should be avoided. Due process, quality of evidence, independence of judiciary, and right to a fair hearing should become the main principles of the justice system.

Lastly, the punishment to be used must fulfill three goals, which include the deterrence goal, safety of the society and rehabilitation of the offenders. In the context of Islamic legal framework, public interest and the prevention of harm are the guiding principles of the framework, pointing to the fact that the principle of proportionality is very crucial (al-Shāṭibī, 1997). Thus, a proper system can be seen as one that protects its users and fulfills the principles of justice, mercy and accountability of Shariah.

6.5 Institutional Accountability

Institutional accountability can be considered one of the key problems in the framework of Sharia-based cyber security in Pakistan. It is impossible to protect the digital sphere only using the personal accountability. Government institutions, financial institutions, universities, hospitals, technology companies, and police are obliged to provide safety for the information which has been entrusted to them. In Islam, there are high standards of amānah (trust). According to the Qur'an, "O you who have believed, fulfill [all] contracts" (Qur'an 4:58). The above-mentioned statement is the basis for all kinds of institutional responsibility in respect of the private information in their possession, which includes private data, financial information, and systems. Hence, institutions need to develop the proper regulations and policies in the field of cyber security, access controls, data protection policy, cyber security education of employees, assessment of the level of cyber security in institutions, and reporting of cyber security events. Otherwise, individuals and institutions will incur losses because of the absence of security. Lā ḍarar wa lā ḍirār stands for the principle of prevention which means the protection of other people from potential harm. The National Cyber Security Policy of Pakistan for 2021 requires coordination between several institutions, capability development, security standards in cyberspace, and vital information systems protection (Government of Pakistan, 2021). The goal can be reached due to such Islamic values as amānah, ʿadl (justice), and mas'ūliyyah (responsibility). Moreover, in case any information leak takes place, institutions have to be transparent in terms of provision of remedial measures to those who have been affected by it. It is worth mentioning that the problem concerns not only the public sector but also the private one. Due to audits, proper cyber security policy, training, and supervision the degree of negligence can be reduced and trust raised from the side of the society. In other words, Shariah-based cyber security policy in institutions is not only technical but also moral and ethical problem.

6.6 Collective Ijtihād

Collective ijtihād is regarded as one of the ways of development of an appropriate Islamic response to modern cyberspace criminality in Pakistan. Modern technologies developed for use in

cyberspace develop at an extremely high pace, thus giving rise to a completely new type of behavior which has never been described in traditional Islamic legal resources before. In particular, such crimes as hacking, ransomware, AI scams, identity theft, cryptocurrency fraud, deepfakes, data breaches, cyber wars need a special knowledge of these technologies and the Islamic legal justification of these actions. It means that it is not enough to solve these problems being an expert in just one field. However, the Islamic legal theory has already developed some methods which could be used in analyzing the newly emerged online crimes. Among them are such methods as qiyās or analogy of reasoning, maṣlaḥah or necessity of action for the sake of public welfare, sadd al-dharāiʿ or blocking the means causing harm and goals of Shariah or maqāṣid al-sharīʿah (al-Shāṭibī, 1997; Kamali, 2008). However, in order to properly implement them, it is necessary to have a thorough understanding of these technologies and the degree of their danger both to people and to society. Therefore, it is reasonable to involve in the process of collective ijtihād representatives of Islamic jurisprudence, legal experts, cybersecurity specialists, software engineers, law-enforcement agents, politicians and digital ethics experts. Such specialists would be able to distinguish the lawful technological practices from the criminal actions and would contribute to the development of the proper legislation and ethical standards. For instance, the cybersecurity specialists would be able to provide technical information regarding hacking, while the Islamic scholars could analyze the case taking into consideration the aspects of the privacy, property, damage, trust, and public welfare violation.

It is reasonable to form advisory boards consisting of experts from universities, religious organizations, governmental institutions, and cybersecurity specialists to analyze the situation regarding the newly emerged cybercrimes in Pakistan. Proposals of these organizations may prove helpful in developing the legislative acts, court decisions, and policies regarding cybersecurity.

Therefore, collective ijtihād will help to create an Islamic response to cybercrimes, which will consider all the essential principles but will keep up with the technological developments.

7. Relationship between PEC Act and Current Pakistani Law on Cybercrime

Currently, the legal regime of Pakistan serves as the foundation for ensuring digital security in this country. The creation of the PEC Act was intended to provide protection against possible violations concerning the information systems as well as establish the processes of investigation, prosecution, trial, and international cooperation. The main objective of the National Cyber Security Policy 2021 is to ensure safety, reliability, and standardization of the process of digital activity and cyber security capacity of the country. Special research has been conducted for the purpose of analyzing the cybercrime legislation of Pakistan and its compliance with the Islamic law requirements. As a result, it was found that all legislative acts comply with modern cyber law requirements (Bilal & Khan, 2022). Therefore, there are no issues of incorporating traditional crimes into the legislation of Pakistan.

8. Conclusion

Cybercrime may be considered one of the most important barriers on the way to digitalization of Pakistan. There are a lot of institutions and laws in the current legislation and national cybersecurity policy of the country, but without creating the ethical framework it is impossible to provide effective digital security. Islam offers such an ethical framework, which includes maqāṣid al-sharīʿah, ʿadl, amānah, maṣlaḥah, right to privacy, verification of information, and prohibition of harm. All modern cybercrimes may be effectively regulated by means of taʿzīr instead of ḥudūd, as taʿzīr provides the government with additional opportunities to punish cybercriminals in case of digitalization. Besides, Islam offers people the necessary information concerning measures which need to be undertaken for protection against any information leakages, safe communication in the digital environment, awareness of cyber security and institutional accountability. It is obvious that the digital security framework based on Shariah should be developed in Pakistan and applied along with existing legislation. This framework should be ethical according to the principles of maqāṣid al-sharīʿah and cybersecurity standards and include appropriate digital evidence, fair punishment, institutional accountability, and ijtihād.

References

Abrar, M. (2026). *Islamic law and cybercrime: Challenges in the digital age*. SSRN. https://ssrn.com/abstract=6455158

Al-Anazi, L. N. B. M. (2026). The rule of harm and its applications to AI crimes. *Journal of Islamic and Religious Studies, 11*(1). https://doi.org/10.36476/JIRS.11:1.06.2026.07

Al-Ghazālī, A. H. (1997). *Al-Mustaṣfā min ʿilm al-uṣūl* [The essentials of Islamic legal theory]. Dār al-Kutub al-ʿIlmiyyah.

Al-Shāṭibī, I. (1997). *Al-Muwāfaqāt fī uṣūl al-sharīʿah* [The concordances on the foundations of Islamic law]. Dār Ibn ʿAffān.

Bilal, H., & Khan, M. A. (2022). Cyber crime legislation in Pakistan: A critical analysis from Islamic law perspective. *Al-Idah, 40*(2), 1–18. https://doi.org/10.37556/al-idah.040.02.0802

Government of Pakistan. (2016). *Prevention of Electronic Crimes Act, 2016*. Pakistan Code. https://www.pakistancode.gov.pk/pdffiles/administrator6a061efe0ed5bd153fa8b79b8eb4cba7.pdf

Government of Pakistan, Ministry of Information Technology and Telecommunication. (2021). *National cyber security policy 2021*. https://pkcert.gov.pk/uploads/2023/06/2021-National-Cyber-Security-Policy-Final.pdf

Ibn Mājah, M. Y. (2007). *Sunan Ibn Mājah*. Darussalam.

Isah, J., Qaser, H., & Zeki, A. M. (2026). Cyber laws and Islamic perspectives on digital ethics. *International Journal on Islamic Applications in Computer Science and Technology, 14*(1). https://ijasat.com/index.php/ijasat_en/article/view/409

Kamali, M. H. (2008). *Shari'ah law: An introduction*. Oneworld Publications.

The Qur'an. (n.d.). *The Holy Qur'an*.