Journal of Information Systems Engineering and Management
2025, 10(24s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The Crime of Cybersecurity Violation from the Perspective of Islamic Jurisprudence and Its Impact on Sustainable Development

Ali Ahmed Salem Farhat[1], Jamal Lakhdar Hammoud Azzoun[2], Ahmed Youssef Saadiya[3]
[1,2]Department of Sharia, College of Sharia, Najran University, Kingdom of Saudi Arabia
[3]Department of Islamic Studies, Faculty of Arts, Taibah University; Kingdom of Saudi Arabia
aafarahat@nu.edu.sa[1], ali.ahmed6405@gmail.com[1] jlazoune@nu.edu.sa[2] and aabdousaadia@taibahu.edu.sa[3]
https://orcid.org/0009-0001-0038-8629[1], https://orcid.org/0009-0008-7464-8930[2] and https://orcid.org/0009-0009-6141-290X[3]

ARTICLE INFO

Received: 16 Dec 2024

Revised: 02 Feb 2025

Accepted: 20 Feb 2025

ABSTRACT

This research aims to elucidate the concept of the crime of cybersecurity violation, its significance, its elements, its penalties, and its causes for exemption, as well as its impact on sustainable development. The study adopts a descriptive approach, relying on an analytical methodology, and has yielded several key findings, the most notable of which are:

Cybersecurity is a system concerned with protecting networks and programmes against attacks that aim to access, alter, or destroy information. The three elements of the crime of cybersecurity violation are: the legal element, the material element, and the mental element, which pertains to the intent of the perpetrator. The primary means of proving the crime of cybersecurity violation include testimony, confession, inspection, and other forms of evidence. All forms of cybersecurity violations are prohibited under Islamic law and are criminalised under Saudi and statutory law. Islamic law is established on the foundation of protecting and preserving security in all its forms and has enacted both Sharia-based and statutory regulations to ensure the continuity of sustainable development.

Key Recommendations:

- Emphasizing the need for researchers to link contemporary crimes to sustainable development.
- Urging statutory and regulatory legislators to impose stricter penalties for cybersecurity violations.

Keywords: Crime – Cyber – Security – Islamic Jurisprudence – Statutory Law.

INTRODUCTION

All praise is due to Allah, as befits His Majesty and Supreme Sovereignty, His encompassing Mercy, and His abundant Bounty. May peace and blessings be upon our Master Muhammad, and upon his family and all his companions.

To begin with

One of the distinctive characteristics of Islamic law is its applicability across all times and places, its flexibility in addressing new challenges and contemporary issues, its ease of implementation, and its ability to apply fixed rulings from the Qur'an and Sunnah to present realities in a manner that aligns with the individual's circumstances and the broader human society.

From this perspective, the present research forms part of a proposed research project encompassing the study of a range of contemporary crimes from a jurisprudential perspective. Experts in the field fully comprehend the gravity of the damage caused by crimes of all kinds, including psychological, health-related, and financial harm, as well as their significant impact on the global economy, striking at the very foundations of sustainable development.

The nation has made remarkable strides in promoting cybersecurity awareness, as evidenced by numerous specialised training programmes and diverse university courses, which stand as testimony to this pioneering effort. This research seeks to elucidate key legislative and regulatory aspects within this field.

Research Problem: The research problem can be formulated in the following primary question: What is the concept of the crime of cybersecurity violation, what are its elements, what are its penalties, and what are its causes for exemption?

Research Objectives: Based on the aforementioned inquiries, the research objectives can be formulated as follows:

- To define and establish the jurisprudential basis for the crime of cybersecurity violation and to identify its elements.
- To clarify the penalty for cybersecurity violation under Islamic jurisprudence, the Saudi law, and statutory law.
- To outline the causes for exemption from the penalty for cybersecurity violation.

Research Methodology: The study adopts an inductive methodology, whereby the subject matter of the research is examined through specialised writings, which analyse and present the issue comprehensively.

Research Plan: The study consists of an introduction, two main topics, a conclusion, and an index, as follows:

Introduction: The introduction addresses the research problem, its objectives, significance, methodology, and structure. It includes two main topics, a conclusion, and a list of references.

Topic One: Definition of the Crime of Cybersecurity Violation

Topic Two: The Penalty for Cybersecurity Violation and Its Causes for Exemption

Topic One: Definition of the Crime of Cybersecurity Violation from the Perspective of Islamic Jurisprudence and the Saudi Law.

The crime of cybersecurity violation falls within the category of electronic crimes, which encompass unlawful activities carried out by specialists in various forms of cybercrime to achieve specific objectives, such as obtaining financial gains or executing acts of sabotage aimed at accessing, altering, or destroying information.

First: The Concept of Crime in Islamic Jurisprudence and Statutory Law

In linguistic terms, "crime" is derived from the Arabic term *jurm*, meaning transgression, and *jurm* also signifies sin, with its plural forms being *ajrām* and *jurūm*. In the Hadith it is stated: *"The worst of the Muslims in terms of crime is the one who asks about something that was not forbidden, so that it becomes forbidden because of his inquiry."*
The phrase "tajarrama alayya fulan" means: "Someone falsely accused me of a crime I did not commit.". The criminal is the offender. [15]

Crime is defined in Islamic law as a prohibited act for which Allah has prescribed either a fixed penalty (ḥadd) or a discretionary penalty (taʿzīr). [1] In legal terminology, a crime is defined as a voluntary act prohibited by law for which the perpetrator is subject to criminal penalty. [9]

From the foregoing, it is evident that both the Islamic and legal definitions of crime conform to the linguistic definition in that a crime is considered a prohibited act; however, the concept of crime in the language is broader than in Sharia and statutory law. [6]

Second: Definition of Cybersecurity

Such terms require careful consideration, with their parameters clarified and their religious rulings explicitly set forth, particularly since these means are inherently dynamic and their issues encompass a range of complexities that lack an established jurisprudential and legal foundation.

"Security" linguistically is antonymous with "fear." [12]

"Cyber" is a term of foreign, specifically Greek, origin; "cyber" pertains to cyberspace and denotes the protection of assets through information technology, such as devices and software. [16] [17]

Second: Definition of the Term Cybersecurity

Cybersecurity is defined as a system concerned with protecting networks and programmes against attacks that aim to access, alter, or destroy information. [16] [17]

Elements of the Crime of Cybersecurity Violation

As is well known, crimes are prohibited under Islamic law, for which Allah has prescribed either a fixed punishment (ḥadd) or a discretionary punishment (taʿzīr), and these prohibitions are those acts that are either committed despite being forbidden or omitted despite being obligatory. We stated that the prohibitions are described as "legitimate" since they must be expressly forbidden by the texts of Sharia, and an act or omission is not in itself a crime unless it is punishable. The elements of the crime of cybersecurity violation are three:

1. There must be a textual prohibition of the crime and a prescribed punishment for it, which in our legal terminology is called the "legal element" of the crime.
2. The commission of the act constituting the crime, whether by action or by omission, which we refer to in legal terminology as the "material element" of the crime.
3. The perpetrator must be accountable, that is, legally responsible for the crime, which is known today as the "mental element" of the crime. [3] [9] [10]

Means of Proving the Crime of Cybersecurity Violation

The means of proving cybersecurity crimes—like all other crimes—consists of establishing that the crime was committed by demonstrating its legal elements and then attributing it to the accused as the perpetrator through what is known as attribution evidence, that is, evidence which establishes his connection to the crime either as the principal actor or as an accomplice, or disproves this connection. This is the field of criminal evidence. [5]

Furthermore, the evidentiary process involves presenting attribution evidence which clarifies the extent of the perpetrator's involvement in the crime, either positively or negatively, whether as a principal actor or as an accomplice through incitement, conspiracy, or assistance, and these are the evidentiary methods upon which the court bases either the conviction or the acquittal of the accused. [9]

Among the most important methods acknowledged by the criminal legislator as means of proving crimes are: testimony, confession, inspection, expert evidence, documentary evidence, circumstantial evidence, and oath-taking, among others. [8]

From the foregoing, it is evident that the evidentiary standard in Islamic criminal law differs from that applied in statutory law. Islamic law has imposed certain conditions which must be met in testimony, and it prescribes a required threshold for such testimony. Moreover, other means of proof—such as confession, written evidence, and oath-taking—are safeguarded by guarantees within Islamic law that ensure the protection of rights, respect for individual freedoms, and the honour of persons. [18]

Topic Two: The Penalty for Cybersecurity Violation and Its Causes for Exemption

We have stated that the crime of cybersecurity violation is among the most severe contemporary offences, through which Saudi security and other security interests are threatened. Accordingly, deterrent regulations have been established to combat such crimes and limit their proliferation, in addition to their prohibition under Islamic law.

The Penalty for Cybersecurity Violation in Islamic Law and the Evidence Thereof

All forms of violation are prohibited under Islamic law, including the violation of the security of information belonging to individuals and institutions.

The evidence for the prohibition of cybersecurity violation is as follows

- Allah Almighty states: "And do not seek to cause corruption on earth. Indeed, Allah does not love the corrupters." (Surah Al-Qasas, 77).
- Allah Almighty also states: "And when he turned away, he strived throughout the land to cause corruption therein and to destroy crops and cattle. And Allah does not love corruption." (Surah Al-Baqarah, 205).

- The Messenger of Allah, peace and blessings be upon him, said: “Your blood, your wealth, and your honour are sacred to one another, just as the sanctity of this day, this month, and this city is sacred.” (Narrated by Al-Bukhari). [22]

Furthermore, cyber-attacks fall clearly under these evidences; namely, the attack on assets, economic sabotage, and the halting of sustainable development, through the manipulation, alteration, or hacking of private information. It also includes the violation of the privacy and personal lives of individuals by disclosing secrets and information about them, and the undertaking of destructive measures, whether on a personal or governmental level. The Prophet, peace and blessings be upon him, said: “There should be neither harm nor reciprocation of harm.” (Narrated by Ibn Majah [23]).

The Penalty for Cybersecurity Violation in the Saudi Law

The Saudi Law addresses the penalty for cybersecurity violation from various perspectives: Royal Decree No. M/17 dated 08/03/1428 AH, and Council of Ministers Resolution No. 79 dated 07/03/1428 AH, establishing the Anti-Cybercrime Law (08/03/1428 AH, corresponding to 27/03/2007 AD). Article Three reads:

Any person who commits any of the following cybercrimes – unauthorized access to an electronic website, or accessing an electronic website for the purpose of altering its design, or damaging it, or modifying it, or seizing its domain name – shall be punished by imprisonment for a term not exceeding one year and/or a fine not exceeding five hundred thousand riyals.

In Article Five: Any person who commits any of the following cybercrimes shall be punished by imprisonment for a term not exceeding four (4) years and/or a fine not exceeding three million (3,000,000) riyals: unauthorised access for the purpose of deleting, erasing, destroying, leaking, damaging, altering, or republishing private data; or by disabling, hindering, obstructing, destroying, erasing, leaking, damaging, or modifying computer programmes or the data contained therein; or by obstructing, confusing, or disabling a service by any means whatsoever. In Article Seven: Any person who commits any of the following cybercrimes shall be punished by imprisonment for a term not exceeding ten (10) years and/or a fine not exceeding five million (5,000,000) riyals: unauthorised access to an electronic website, or to an information system either directly, via the information network, or via any computer device, for the purpose of obtaining data that affects the internal or external security of the state or its national economy. [20]

In the Egyptian Penal Code: Article (20) of Law No. 175 of 2018 concerning the Combat of Information Technology Crimes provides that any person who breaches a website, an email account, a private account, or an information system, or who does so on behalf of the state or any public legal entity, or that is owned by or pertains to the state, shall be punished by imprisonment for a term not less than two (2) years and a fine not less than fifty thousand (50,000) Egyptian pounds and not exceeding two hundred thousand (200,000) Egyptian pounds, or by either of these penalties. [21]

It is evident that there is consensus between Islamic jurisprudence and statutory law that a penalty must be imposed upon anyone who commits a cybersecurity violation, although Sharia classifies such individuals among those who cause corruption on earth, whereas statutory law punishes them by imprisonment and the maximum fine, in addition to the disruption they cause to the process of sustainable development.

It may be appropriate in the coming periods to expand the use of technology to support this field (Ahmed, Alharbi, & Elfeky, 2022; Elbyaly & Elfeky, 2023a, 2023c, 2023e, 2023f, 2023g, 2023h, 2023i; A. Elfeky, 2017; A. I. M. Elfeky & Elbyaly, 2016, 2019, 2023a, 2023b, 2023c, 2023e, 2023f, 2023g; A. I. M. Elfeky, Najmi, & Elbyaly, 2023, 2024a, 2024b; Elfekyand, 2016; Masada, 2017; Masadeh & Elfeky, 2016).

Causes for Exemption from the Penalty for the Crime of Cybersecurity Violation

The Causes for Exemption from the penalty for this crime under Islamic jurisprudence are: death, repentance, pardon, and the statute of limitations. In contrast, under statutory law, the grounds for exemption are three: the death of the convicted person, pardon, and the statute of limitations.

First: Death of the Convicted Person: The penalty is waived upon the death of the convicted person, and its enforcement is suspended; however, any financial penalties, compensations, or costs included in the judgement shall be enforced against the deceased’s estate. [10]

Second: Pardon: Pardon is defined as the relinquishment by society of all or some of its rights arising from the crime, and pardon from penalty is the termination by the state of the convicted person's obligation to serve all or part of the sentence. [10]

Third: Statute of Limitations: In law, the Statute of Limitations refers to the lapse of a period specified by law, beginning from the date the final judgement is issued, during which no execution procedures are undertaken. Thus, the Statute of Limitations is its termination after a specified period determined by law, starting from the date the right to its execution arises. [19]

The rationale for the waiver of the penalty due to the statute of limitations is that enforcing the punishment after such a period does not achieve any of its objectives. It aims to achieve justice and benefit, and the accused has already faced his punishment by remaining out of sight for the duration. Moreover, there is no societal interest in executing the punishment once the crime has been effaced. [17]

Furthermore, it has become clear that there are four reasons for the annulment of punishment for this crime in Islamic jurisprudence: death, repentance, pardon, and the statute of limitations. In statutory law, the reasons for annulment of punishment are three: the death of the convicted person, pardon, and the statute of limitations.

It has been observed that the law aligns with Islamic jurisprudence in that financial penalties do not expire upon death, as the financial penalty can be claimed from the estate. Similarly, the law agrees with Islamic jurisprudence in the expiration of punishment by the pardon of the ruler if it is deemed beneficial. [3]

In conclusion,

if sustainable development is defined as the enhancement of production levels through the adoption of the most effective means to achieve optimal investment in clean technology industries that utilise the minimum possible amount of energy, while simultaneously upholding the principles of justice in production and consumption in order to secure the welfare of all members of society without inflicting harm upon nature or the interests of future generations, [4] then this necessitates a degree of security – including cybersecurity. We affirm that Islamic law has been founded upon the protection of security and has enacted both religious legislation and regulatory controls to ensure its preservation.

CONCLUSION

The study has reached several key findings, the most notable of which are as follows:

- Cybersecurity: A system concerned with protecting networks and programmes against attacks intended to access, alter, or destroy information.
- The elements of the crime of cybersecurity violation are three: the existence of a textual prohibition of the crime; the material element; and the accountability of the perpetrator, that is, the mental element.
- Islamic jurisprudence and statutory law concur that a penalty must be imposed on anyone who commits an attack on cybersecurity, although Sharia classifies such individuals among those who corrupt the earth, whereas statutory law imposes imprisonment and the maximum fine as punishment for their offences.
- Cybersecurity is safeguarded by Islamic law, which has enacted both Sharia-based and statutory legislation to ensure the preservation of sustainable development.
- The penalty for this crime under Islamic jurisprudence is waived in cases of death, repentance, pardon, and the statute of limitations, while under statutory law the grounds for exemption are three: the death of the convicted person, pardon, and the statute of limitations.

RECOMMENDATIONS

- Researchers should be urged to link contemporary crimes to sustainable development.
- The penalties for attacks on cybersecurity should be increased.

ACKNOWLEDGMENT

The authors are thankful to the Deanship of Graduate Studies and Scientific Research at Najran University for funding this work under the Growth Funding Program grant code (NU/GP/SEHRC/13/72-1).

REFERENCES

[1] Judiciary and Authority, Abu Al-Hassan Al-Mawardi, 3rd ed., (Beirut: Dar Al-Kotob Al-Ilmiyyah, 2006).

[2] Authentication of Enforcement Procedures, Abdul Fattah Mustafa Al-Sayfi, d.t., (Alexandria: Dar Al-Huda, 2002).

[3] Sharia Judiciary Compared to Positive Law, Abdul Qader Al-Awda, 14th ed., (Al-Risalah Foundation, 1418-1997 AD Beirut).

[4] Scientific Development (Its Concept - Dimensions - Indicator) Medhat Abu Al-Nasr, Yassin Muhammad, d.t., Cairo Publisher: Arab Group for Training and Publishing, 2017.

[5] Prove It with the Basic Principles of Science, Distinctive Evidence in the Field of Proving It, Abu Bakr Abdul Latif, d.t., (Riyadh: Dar Al-Marikh, 1415-1995 AD).

[6] Crime and its General Charge in Modern Editions and Islamic Jurisprudence, Osama Abdullah Qaid, 2nd ed., (Cairo: Dar Al Nahda, 1995).

[7] Ahmed, E. S. A. H., Alharbi, S. M., & Elfeky, A. I. (2022). Effectiveness of a proposed training program in developing twenty-first century skills and creative teaching skills among female student teachers, specializing in early childhood. *Journal of Positive School Psychology*, 4316-4330.

[8] Masadeh, T. S. Y., & Elfeky, A. I. M. (2016). Efficacy of open-source learning management systems in developing the teaching skills of English language student teachers. *American Journal of Educational Research*, *4*(4), 329-337.

[9] Masada, T. S. Y. (2017). Immediate versus delayed feedback in promoting student teachers skills for lesson plan implementation. *Thouqan Saleem Yakoub Masadeh and Abdellah Ibrahim Mohammed Elfeky (2017) Immediate Versus Delayed Feedback in Promoting Student Teachers Skills for Lesson Plan Implementation, British Journal of Education*, *5*(8), 43-58.

[10] Elfeky, A. I. M., & Elbyaly, M. Y. H. (2016). The impact of learning object repository (lor) in the development of pattern making skills of home economics students. *British Journal of Education*, *4*(2), 87-99.

[11] Elfeky, A. I. M., & Elbyaly, M. Y. H. (2023). The effectiveness of virtual classrooms in developing academic motivation across gender groups. *Ann. For. Res*, *66*(1), 2005-2020.

[12] Elfekyand, A. I. M. (2016). The use of CSCL environment to promote students' achievement and skills in handmade embroidery. *Journal of Home Economics*, *26*(3).

[13] Elfeky, A. I. M., & Elbyaly, M. Y. H. (2023). The impact of virtual classrooms on the development of digital application skills among teachers of digital skills in Najran region. *Ann. For. Res*, *66*(1), 2044-2056.

[14] Elbyaly, M. Y. H., & Elfeky, A. I. M. (2023). The impact of blended learning in enhancing the skill performance of producing digital content among students of optimal investment. *Ann. For. Res*, *66*(1), 2031-2043.

[15] Elfeky, A. (2017, July). Social Networks Impact factor on Students' Achievements and Attitudes towards the" Computer in Teaching" Course at the College of Education. In *International journal on E-learning* (Vol. 16, No. 3, pp. 231-244). Association for the Advancement of Computing in Education (AACE).

[16] Elfeky, A. I. M., & Elbyaly, M. Y. H. (2023). Examining the effects of virtual classroom use inside learning management systems on enhancing student satisfaction. *Ann. For. Res*, *66*(1), 1980-1990.

[17] Elbyaly, M. Y. H., & Elfeky, A. I. M. (2023). The effectiveness of a program based on augmented reality on enhancing the skills of solving complex problems among students of the Optimal Investment Diploma. *Annals of Forest Research*, *66*(1), 1569-1583.

[18] Elfeky, A. I. M., & Elbyaly, M. Y. H. (2019). Multimedia: different processes. In *Interactive multimedia-multimedia production and digital storytelling*. IntechOpen.

[19] Elbyaly, M. Y. H., & Elfeky, A. I. M. (2023). The impact of problem-solving programs in developing critical thinking skills. *European Chemical Bulletin*, *12*, 6636-6642.

[20] Elfeky, A. I. M., Najmi, A. H., & Elbyaly, M. Y. H. (2023). The effect of big data technologies usage on social competence. *PeerJ Computer Science*, *9*, e1691.

[21] Elfeky, A. I. M., & Elbyaly, M. Y. H. (2023). THE EFFECT OF E-TUTORIAL PROGRAMS ON IMPROVING THE PRODUCING DIGITAL CONTENT SKILL. *European Chemical Bulletin*, *12*, 6581-6587.

[22] Elfeky, A. I. M., & Elbyaly, M. Y. H. (2023). The Impact Of Project-Based Learning On The Development Of Cognitive Achievement In The Course Of Applications In Educational Technology Among Students Of The College Of Education At Najran University. *European Chemical Bulletin*, *12*(6), 6643-48.
[23] Elbyaly, M. Y. H., & Elfeky, A. I. M. (2023). Collaborative e-learning environment: Enhancing the attitudes of optimal investment diploma students towards the digital skills course. *European Chemical Bulletin*, *12*, 6552-6558.
[24] Elbyaly, M. Y. H., & Elfeky, A. I. M. (2023). The Effectiveness of Using Advanced Organizations within the Virtual Classroom to Enhance the Acceptance of Technology During Disasters. *European Chemical Bulletin*, *12*, 6603-6612.
[25] Elbyaly, M. Y. H., & Elfeky, A. I. M. (2023). The Efficiency of Online Learning Environments In Fostering Academic Motivation. *European Chemical Bulletin*, *12*, 6622-6628.
[26] Elbyaly, M. Y. H., & Elfeky, A. I. M. (2023). The efficiency of instructional gaming programs in stimulating creative thinking. *European Chemical Bulletin*, *12*, 6613-6621.
[27] Elfeky, A. I. M., & Elbyaly, M. Y. H. (2023). MANAGING DRILL AND PRACTICE PROGRAMS WITH A MOTIVATIONAL DESIGN AND THEIR EFFECTS ON IMPROVING STUDENTS'ATTITUDES TOWARD INFORMATION AND COMMUNICATION TECHNOLOGY COURSES. *European Chemical Bulletin*, *12*(6), 6567-6574.
[28] Explanation of the General Instructions for the Special Procedures of Law 145 of 2006 and Law No. 74 and 153 of 2007.
[29] Explanation of the General Instructions for the Special Procedures of Law 145 of 2006 and Law No. 74 and 153 of 2007.
[30] Explanation of the Crime Law, Part Two, Public Harm, Ali Abdel Qader Al-Qahwaji, and Fattouh Abdullah Al-Shazly, (Alexandria: Dar Al-Huda for Publications, 2002).
[31] Explanation of the Penal Code, General Section, Mahmoud Mahmoud Mustafa, 10th ed., (Cairo: Dar Al-Nahda Al-Arabiya, 1983).
[32] Al-Ain, Al-Khalil Al-Farahidi Al-Basri, Publisher: Dar and Library of Al-Hilal.
[33] Criminal Law, its Procedures, Muhammad Muhyi al-Din Awad, (Cairo University Press, 1981), pp. 678-679.
[34] Criminal Penal Code, Chapter Sixteen, Article (375) bis, added by Law No. (10) Final (2011).
[35] Lisan al-Arab, Ibn al-Khattab al-Afriqi, Publisher: Dar Sadir - Beirut, Third Edition - 1414 AH
[36] Pioneer in Cybernetics, Muhammad Awad, State of Qatar (Security Training Course).
[37] Introduction to the Book of Cybernetics Translated, Hussam al-Din 2017 AD, Taiba Security University.
[38] The Comprehensive Encyclopedia of Criminal Statute of Limitations, Hisham Zuwain, Volume One, 3rd Edition, (Cairo: Mahmoud Center for Legal Publications, 2010).
[39] The Theory of Evidence in Islamic Jurisprudence, Ahmed Fathi Bahnasy, 5th ed., (Cairo: Dar Al-Shorouk, 1409-1989).
[40] General Response to Punishment, Abdel-Baqi Al-Sagheer, d.t., (Cairo: Dar Al-Nahda Al-Arabiya, 1997).
[41] Saudi Council of Ministers Experts Authority https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/1?csrt=4284193624993328879
[42] Corruption Publications https://manshurat.org/node/31487
[43] Sahih Al-Bukhari, Muhammad bin Ismail Abu Abdullah Al-Bukhari Al-Ja'fi, 1st ed., Lebanon, Dar Tawq Al-Najat, 1422 AH.
[44] Sunan Ibn Majah Sunan Ibn Majah, Muhammad bin Yazid Abu Abdullah al-Qazwini, edited by: Muhammad Fuad Abdul-Mutabaqi, 1st ed., Beirut, Dar al-Fikr, n.d.