Application of the Concept of Probative Value in Cyber Shariah Criminal Cases

Najeehah Hana' binti Nasiruddin[1], Mohamad Azhan Yahya[2], Mohd Izzat Amsyar Mohd Arif[3], Ahmad Azam Mohd Shariff[4], Mohamad Rizal Abd Rahman[5], Mohd Sabree Nasri[6]

[1,2,3]Undergraduate Student, Faculty of Law, University Kebangsaan Malaysia,

[4]Legal Advisor, Afandi Dahari & Associates, Selangor, Malaysia,

[5]Associate Professor, Faculty of Law, University Kebangsaan Malaysia,.

[6]Lecturer, Faculty of Law, Governance and International Relations

DOI: https://dx.doi.org/10.47772/IJRISS.2025.909000735

Received: 24 September 2025; Accepted: 29 September 2025; Published: 28 October 2025

ABSTRACT

This article examines the application of the concept of probative value in Syariah criminal cases involving social media. With the rapid advancement of technology and the widespread use of social media, digital evidence has become increasingly important in judicial processes. In the context of Syariah criminal cases, evidence from social media must be evaluated in terms of authenticity and admissibility according to Syariah principles. This article discusses how probative value, which is the ability of evidence to prove a particular fact, is applied in these cases. The study also explores the challenges faced by the Syariah legal system in handling digital evidence and provides recommendations for improving the evaluation process of such evidence. The findings indicate that a more systematic approach and broader recognition of digital evidence are needed to ensure justice in Syariah criminal cases in this digital age. Furthermore, the article outlines several measures that can be taken by authorities to increase awareness and understanding of the importance of digital evidence among the parties involved. These measures include the amendment of current law, and the application of a standard operating procedure (SOP) to govern Syariah criminal cases that occur in social media. The article emphasizes that to achieve comprehensive justice, the evaluation of digital evidence must be conducted meticulously and based on robust Sharia principles. Considering the evolving technological landscape, the article also calls for relevant legal reforms to address the issues arising from digital technological advancements.

Keywords— probative value; shariah; digital; electronic document evidence; proof.

INTRODUCTION

In the rapidly developing digital age, Shariah criminal offences are no longer limited to the physical sphere but have also extended into cyberspace. This refers to the violation of Islamic principles and laws through the use of information and communication technology including social media, websites and other digital platforms. Technological advancement has created both new opportunities and challenges in complying with Shariah law where individuals have the freedom to either spread good or misuse the digital space for purposes that are contrary to Islamic principles.

Among the types of Shariah offences committed in cyberspace are insults against Islam, the dissemination of slander, incitement against Islamic institutions and the distribution of obscene content and online gambling. For example, in the case of Chiok Wai Loong, a social application technician who was sentenced to imprisonment and fined for posting offensive content relating to the word 'Allah', it clearly illustrates that the misuse of cyberspace can lead to serious criminal offences under both civil and Shariah law (Faris Fuad 2024).

In the context of proof, electronic evidence plays a vital role in Shariah criminal cases that occur online.

Electronic documents encompass any form of information that is created, stored or transmitted through electronic devices such as smartphones, computers, hard drives or internet networks. According to Muhammad Fawwaz (2008), an electronic document is a note or any material that can be understood and clearly viewed when processed by electronic equipment. In addition, Mohamad Ismail Hj. Mohamad Yunus (2006) states that sources of electronic evidence involve various media including VLSI chips, storage devices, computer software and digital communication systems.

Nevertheless, in order to ensure the admissibility and effectiveness of electronic evidence in Shariah trials, aspects of probative value such as truthfulness, integrity and relevance must be carefully assessed. The collection or presentation of electronic evidence that is unlawful or that fails to adhere to principles of justice may compromise the rights of the accused and violate the maqasid al-Shariah which emphasizes justice, truth and the protection of rights.

Therefore, this article aims to discuss the application of the concept of probative value in the context of electronic evidence in Shariah criminal cases in cyberspace by assessing its admissibility, authenticity and appropriateness from the perspective of Islamic legal theory and contemporary legal practice.

RESEARCH METHODOLOGY

In order to achieve the research objectives, the chosen methodological approach must align with the scope and research questions raised. Therefore, this study adopts a pure legal research methodology that is doctrinal and qualitative in nature to examine in depth the principles and legal provisions related to the probative value of electronic evidence in Shariah criminal cases in cyberspace. Pure legal research refers to an inquiry aimed at understanding, analysing and interpreting existing laws within a legal system particularly within the context of Shariah. This approach is considered the most appropriate as the main focus of the study is the analysis of legal principles and the effectiveness of the legal framework in addressing contemporary legal issues concerning electronic evidence in Shariah criminal proceedings (Kamel Adibah and Azhan 2021).

This research relies on two main types of sources namely primary data and secondary data. Primary sources consist of statutes, state Shariah enactments and court cases related to the issue of electronic evidence. Secondary sources include academic books, journal articles, theses and relevant research reports. The data collection technique is carried out through library-based research which involves the process of searching collecting and critically evaluating relevant literature in both printed and digital forms. Among the key works referred to are the article "Analysis Proses Pengumpulan Keterangan Dokumen Elektronik dalam Kes Jenayah Syariah" (2021) by Mohamad Azhan Yahya Hammad Mohamad Dahalan and Suhaizad Saifuddin the article "Keterangan Dokumen Dalam Bentuk Digital Di Mahkamah Syariah: Analysis Berkaitan Definisi Serta Kebolehterimaannya Di Sisi Prinsip Syariah Di Malaysia" (2017) by Mohamad Azhan Yahya Ahmad Azam Mohd Shariff and Mohd Abu Hassan Abdullah as well as several other works such as those by Ramalinggam Rajamanickam Nur Insyirah Mohamad Noh and Anita Harun (2022) and by Mohd Sabree Nasri and Ruzman Md Noor (2020) which discuss expert opinion and the evidentiary process in Shariah cybercrime cases.

The data obtained from library sources are analysed through legal content analysis by evaluating the admissibility relevance and integrity of electronic evidence based on Shariah legal principles and current legal practices. In this context attention is given to how principles such as *al-'adalah* and *al-haqq* are applied in the evaluation of digital evidence and the extent to which these principles support the validity of evidence in the Shariah courts. Through this approach the study aims to provide a holistic perspective on the admissibility of electronic evidence in Shariah criminal cases and to contribute to the improvement of the Islamic legal system in line with the challenges of the current digital era.

RESEARCH FINDINGS

Shariah Principles and Probative Value

In this context, it is essential to understand how Islamic legal principles interact with modern legal concepts such as probative value in assessing the reliability of digital evidence in Shariah criminal cases in cyberspace.

Probative value is the criterion used to determine the strength or reliability of a piece of evidence in judicial proceedings. This value plays a crucial role in the evaluation of electronic evidence such as text messages, emails or websites which require careful assessment of authenticity, integrity and relevance.

The concept of probative value is important to ensure that only valid and sufficiently reliable evidence is admitted during trial. According to Ibn Taymiyyah (2001) and Ibn Qayyim (1996), evidence is defined as "anything that reveals and manifests the truth." Therefore, it is appropriate to accept all legitimate methods of uncovering the truth as admissible evidence in court.

According to Informant 1 (personal communication 11 April 2018), probative value refers to the need for a high level of confidence in a piece of evidence. Informant 2 (personal communication 9 July 2018) stated that the evidence must be sufficient to substantiate a claim or argument. Informant 3 (personal communication 2 May 2018) emphasized the importance of evidentiary chains which refer to the linkages among individual pieces of evidence that form a valid conclusion. Meanwhile, the chain of custody refers to efforts to maintain the strength and integrity of the evidence including the credibility of witnesses and the preservation of documents (Informant 4 personal communication 29 January 2018).

In Shariah criminal law there are two main methods of proof which are iqrar and shahadah. Ikrar refers to an admission of an act or liability made in writing orally or through gestures and is accepted as evidence in all types of cases (Section 17(1), Syariah Court Evidence (Federal Territories) Act 1997). Shahadah refers to oral testimony in court delivered using specific phrases to establish a right or interest (Section 3, Syariah Court Evidence (Federal Territories) Act 1997; Abd al-Mutalib Abd Razak Hamdan 2007).

Islamic legal principles such as justice and truth serve as fundamental pillars in the Islamic legal system and must be integrated in the collection of digital evidence. In this regard the burden of proof must be borne by the claiming party and facts must be proven with relevant and valid evidence.

In line with the objectives of Shariah the need to protect public welfare includes the safeguarding of religion life intellect lineage and property. Therefore, the process of investigation and the collection of digital evidence must be adapted to Shariah principles including relevance admissibility probative value corroborative value and the chain of custody and evidence.

In addition the fiqh principle "certainty is not overruled by doubt" (Abd Latif Muda and Rosmawati Ali 2000) is also relevant. It states that something certain should not be invalidated merely due to the presence of doubt. In the context of digital evidence if forensic support and witness confirmation exist then unsubstantiated doubts should not negate the admissibility of the evidence.

Recommended font sizes are shown in Table 1.

Shariah Legal Provisions

Shariah law in Malaysia specifically regulates the procedures and types of evidence that may be admitted in the Shariah courts. In this context documentary evidence and the power of search granted to religious enforcement officers play a significant role. These legal provisions ensure that the evidence presented is valid and obtained through proper procedures thereby safeguarding justice in Shariah court proceedings.

Part II Chapter 3 of the Syariah Court Evidence Enactment (State of Selangor) 2003 places particular emphasis on documentary evidence in Shariah proceedings. Section 49 specifically addresses the concept of primary evidence. Primary evidence refers to the original document or a direct copy obtained from that original. This means that for a document to be accepted as primary evidence it must either be the original version that was issued or a copy that has been directly produced from the original document. Primary evidence is regarded as the most authentic and credible form of proof because it constitutes the original source containing the actual information required in a case. By ensuring that only original documents or direct copies are accepted as primary evidence the court can uphold the accuracy and authenticity of the evidence presented in Shariah proceedings.

In addition Section 63 of the Syariah Criminal Procedure Enactment (State of Selangor) 2003 empowers Religious Enforcement Officers to conduct or authorise searches if they believe that the production of a document or other item is necessary for the investigation of a Shariah offence. If there is reason to believe that the individual served with a summons or order is unlikely to comply with it or if the whereabouts of the relevant document or item is unknown the officer is authorized to conduct a search at any relevant location. If it is not feasible for the officer to carry out the search personally, they may instruct a subordinate officer to do so by issuing a written order that specifies the document or item sought as well as the premises to be searched. This provision also states that a search warrant will apply as far as possible to any search conducted under this section. This is particularly important in a study on the application of the concept of probative value in Shariah cybercrime cases as it illustrates the authority granted to law enforcement officers to obtain relevant electronic evidence for the investigation of cyber-related offences.

Overall, the legal provisions related to evidence and search procedures within the Shariah legal system reflect a commitment to justice and transparency. With clear guidelines enforcement officers can carry out their responsibilities more effectively while parties involved in proceedings can ensure that their rights are protected. This forms a fundamental basis for upholding the law and ensuring justice in every case brought before the court.

Civil Legal Provisions

Within the Malaysian civil legal system, specific laws govern the procedures through which documents required for investigation or inquiry may be obtained. This process involves orders issued by a judge or a competent authority to ensure that essential documents can be accessed for judicial purposes. In addition, the law grants the Public Prosecutor the power to authorise searches and the temporary seizure of documents pending the outcome of judicial proceedings.

Furthermore, the Evidence Act 1950 (Act 56) provides the legal framework for the admissibility of electronic evidence in both criminal and civil proceedings before the courts. Section 90A and Section 114A of the Evidence Act 1950 are key provisions that allow for the production and admission of electronic documents as evidence in court. Section 90A stipulates that documents produced by a computer along with the statements contained therein may be accepted as evidence of the facts stated in them if the documents were produced in the ordinary course of computer use. These documents may be admissible whether generated before or after the commencement of the criminal or civil proceedings provided that they were produced during the normal course of usage. This section sets out specific conditions that must be fulfilled to establish the admissibility of electronic documents.

Section 114A enables the court to make reasonable presumptions concerning certain facts in particular cases. For instance, the court may presume that a person found in possession of stolen goods soon after the theft is either the thief or someone who knowingly received the stolen property unless the person can satisfactorily explain how the items came into their possession. This demonstrates that Section 114A grants the court broad authority to draw inferences and conclusions based on the facts and evidence presented. As such Section 114A is also relevant in evaluating the admissibility and probative value of electronic documents in judicial proceedings where the court may exercise this power to make reasonable presumptions about the reliability of the electronic evidence submitted.

Overall, the procedures governing the acquisition of relevant documents and items play a critical role in ensuring the effectiveness of investigations and trials. By providing a clear and structured mechanism the civil legal system ensures that necessary evidence can be lawfully and fairly obtained and processed. This is a key element in upholding justice and preserving the integrity of the judicial process. The civil legal system may also serve as a benchmark for the Shariah legal system to develop more detailed enforcement mechanisms in relation to the admissibility of electronic evidence in court.

Scenarios Relating to the Application of the Concept of Probative Value in Malasian Cases

The findings of this study which link the admissibility of electronic documents in civil courts with the need to recognise digital evidence in the Shariah courts represent a progressive development that warrants attention. This

is in line with the technological realities of the present era which influence the form and type of evidence submitted in judicial proceedings.

Civil courts have demonstrated openness towards digital evidence as reflected in the cases of Munah Bte Ali v Public Prosecutor and Public Prosecutor v Jawan Empaling where the court accepted video recordings and voice recordings as evidence by referring to the definition of "document" in Section 3 of the Evidence Act 1950. This definition has been expanded to include all forms of information recorded or stored electronically (Evidence Act 1950 s.3) reflecting the legal principle of adaptability in keeping with the evolution of technology.

This position is further reinforced in the case of Ahmad Najib bin Aris v Public Prosecutor where the Federal Court affirmed that CCTV recordings and chemical reports generated by a computer may be admitted as evidence if they comply with the requirements of Section 90A of the Evidence Act 1950. Compliance with this provision includes verifying that the computer system was operating properly free from external interference and that the documents were produced through routine use of the system (Evidence Act 1950 s.90A(2)). The emphasis on the integrity and authenticity of the evidence illustrates that the probative value of electronic documents does not lie solely in their existence but depends significantly on the manner in which they were generated.

Furthermore in Mohd Ali Jaafar v Public Prosecutor the Court of Appeal admitted audio recordings of the accused's conversation as the principal evidence in a corruption conviction after their authenticity was verified. The court held that such evidence possessed high probative value and played a vital role in proving the prosecution's case (Mohd Ali Jaafar v Public Prosecutor [2006] 3 MLJ 184). This affirms that electronic documents are not merely supporting evidence but may constitute primary evidence if their authenticity can be established.

In the context of Shariah courts the case of Moriazi bin Muhammad v Ajmawati binti Atan illustrates that the Shariah High Court accepted evidence in the form of cheques and bank receipts in a divorce claim despite the absence of direct witness testimony. The acceptance of such evidence demonstrates the Shariah court's willingness to accord probative value to digital documents based on rational and reasonable evidentiary evaluation.

According to Wan Abdul Fattah Wan Ismail (2013) digital documents have the potential to serve as more stable and consistent forms of evidence compared to oral testimony which is vulnerable to memory lapses or manipulation. However, he emphasised that the authenticity of such documents must be supported by auxiliary mechanisms such as verification by third parties or digital forensic experts. This aligns with the principle of qarinah which is accepted in Islamic law as a form of corroborative evidence especially in cases that do not reach the level of definitive proof such as testimony or confession.

Based on the findings and case examples discussed it is clear that the probative value of electronic documents is recognised within the Malaysian legal system including the Shariah courts provided that standards of authenticity integrity and reliability are met. Moreover, this recognition is consistent with the objectives of Shariah which emphasise justice the prevention of crime and the protection of individual rights thereby enhancing the credibility of the Shariah courts in the digital age.

Therefore, the adaptation of the Shariah legal system to the demands of digital evidence is not merely a matter of choice but a pressing necessity to ensure that justice is comprehensively upheld in cybercrime cases.

Issues In Applying the Concept of Probative Value in Malaysian Cases

The application of the concept of probative value in Malaysian cases presents several challenges related to the acceptance and use of electronic evidence in the Shariah courts. Section 3 of the Syariah Court Evidence (Federal Territories) Act 1997 stipulates that any statement made or described through an object or device is considered a document. Meanwhile Section 49 of the same Act classifies computers as primary evidence meaning that documents produced by computers are accepted as primary evidence. This provision recognizes electronic documentary evidence in certain cases without restriction. This concept has been adapted from the Evidence Act 1950 which has long been accepted in the civil courts. Nevertheless there remain gaps in the law that hinder

effective implementation especially in the context of investigating Shariah criminal offences committed in cyberspace.

One of the main issues concerns the admissibility of electronic evidence as valid proof in the Shariah courts due to a lack of legal provisions addressing the use of technology within the framework of Shariah law. A significant challenge arises regarding the authenticity of the electronic document itself. The difficulty in assessing electronic evidence stems from its vulnerability to alteration copying or deletion. For instance in the case of Alliance and Leicester Building Society v Ghahremani the court found that electronic evidence could be manipulated including changes to the date or calendar on a computer to reflect a specific time. This raised doubts regarding the authenticity of the evidence as forensic data analysis revealed empty space on the diskettes used which ultimately led the court to exclude the evidence.

Another issue related to electronic evidence is whether it should be classified as physical evidence in determining the appropriate mode of proof. Electronic evidence is considered valid and admissible in court either as documentary or physical evidence. According to Sybil Sharpe in her book Electronically Recorded Evidence: A Guide to the Use of Tape and Video Recordings in Criminal and Civil Proceedings if the content of the electronic material is central to the case it is considered documentary evidence whereas if it is not central it is regarded as physical evidence. In R.M. Malkani v State of Maharashtra Justice Ray held that when electronic material is used as evidence for evaluation it is deemed relevant to the case and may be admissible regardless of whether it is classified as documentary or physical.

Additionally, another key issue is whether electronic evidence should be accepted as primary or secondary evidence. In Rama Reddy v V.V. Giri Justice Vitiating stated that electronic evidence constitutes primary evidence for purposes of corroboration or contradiction. This opinion highlights the critical role of electronic evidence in ensuring factual accuracy and truth in a case. In R. v Maqsud Ali Justice Marshall stressed that electronic evidence must be received cautiously depending on the factual circumstances of the case. However, in Taylor v Chief Constable of Cheshire Justice Ralph Gibson opined that electronic evidence should be treated on par with other types of evidence without undue emphasis.

There are also challenges related to the jurisdiction of the courts in accepting or rejecting electronic evidence. In Maqsud Ali Justice Marshall stated that the court has the discretion to admit or reject electronic evidence depending on its strength transparency and credibility. Electronic evidence that carries uncertainty or signs of manipulation should be rejected while evidence that is strong and free from fabrication or interference may be accepted.

Another issue that arises is whether a separate trial is required to determine the authenticity of electronic evidence before it can be admitted in court. In some cases such as Z.B. Bukhari v B.R. Mehra the Supreme Court of India established criteria for assessing the authenticity of electronic evidence but did not require a separate trial. This indicates that separate proceedings are not always necessary in practice.

An additional concern involves recordings made without the knowledge or consent of the accused. In Yusufali v State of Maharashtra the accused objected to the use of a recording made without his consent. However, Justice Bachawat ruled that the recording was admissible as it was voluntarily made and did not affect the authenticity of the evidence. This shows that electronic evidence obtained without the accused's knowledge may still be accepted in court if it meets the required standards of authenticity.

Although there are cases where electronic evidence has been manipulated and excluded this does not mean that all electronic evidence should be categorically rejected in legal proceedings. Islamic legal principles offer guidance to ensure the authenticity of electronic documents before they are admitted as evidence. Therefore, there is a need for specific criteria and evaluation methods that allow the use of technology without compromising the principles of justice and truth in Shariah. One such method is the involvement of experts particularly in the field of digital forensics. In this respect both the Quran and Sunnah emphasise the importance of consulting experts. As stated in Surah Al-Anbiya verse 7:

"And We did not send before you except men to whom We revealed Our message. So ask the people of

knowledge if you do not know." (Al-Qur'an Al-Anbiya 21:7)

Here the term Ahl al-Dhikr refers to those who possess knowledge. The existence of digital forensic experts in Malaysia who are responsible for verifying the authenticity of electronic evidence plays a crucial role in ensuring that the evidence presented is valid satisfies Shariah requirements and is admissible during trial.

Comparative Insights and Future Directions

While the reliance on Malaysian statutes and case law provides a solid foundation, the scope of this study remains somewhat limited as it does not fully engage with comparative experiences from other Islamic jurisdictions. In countries such as Indonesia and Brunei, Syariah courts have increasingly faced challenges in cybercrime adjudication, including the admissibility of electronic records, encrypted communications, and evidence hosted on foreign servers. Similarly, several Middle Eastern jurisdictions, particularly the United Arab Emirates and Saudi Arabia, have begun experimenting with integrated e-court systems and digital forensic standards that offer valuable lessons for Malaysia. Incorporating these comparative insights would allow for a broader appreciation of how Shariah principles are reconciled with the technological complexities of cyberspace.

Another limitation is the underexploration of technical issues that directly affect the probative value of digital evidence. Matters such as verifying metadata, ensuring encryption integrity, cross-border data requests, and maintaining an unbroken digital chain of custody are central to the reliability of electronic evidence. Without addressing these aspects, the probative value framework risks remaining overly theoretical and less applicable to real-world cases. Future research should therefore include interdisciplinary perspectives, particularly from the fields of digital forensics and information security, to strengthen the practical relevance of probative value analysis in Syariah courts.

Recommendations should also extend beyond statutory reform to cover capacity-building measures. Judicial officers, prosecutors, and enforcement agencies require specialised training in handling digital evidence, particularly in identifying manipulation, applying forensic audit techniques, and assessing authenticity through emerging tools such as blockchain verification. Standardised SOPs for evidence handling in cyberspace should be developed at the national level to ensure consistency across jurisdictions. Furthermore, collaborative mechanisms between Syariah courts, civil courts, and IT experts would facilitate a more holistic approach, ensuring that the probative value of digital evidence is applied in a manner that is both legally robust and technologically sound.

By expanding the discussion to include comparative models, technical safeguards, and interdisciplinary training, the application of probative value in Syariah cybercrime cases will become more consistent, practical, and aligned with the evolving realities of digital technology.

CONCLUSION

In assessing the probative value of electronic documents the Shariah courts must consider several crucial factors to ensure that such evidence meets the requirements of Shariah law particularly in relation to the secure transmission and storage of information and the potential risks of manipulation or error. The cases discussed from the Malaysian Civil Courts offer a viable model that can be adopted by the Shariah courts to approach digital evidence in a manner that preserves the integrity of the judicial process while embracing technological advancement. This approach can be adapted by Shariah courts to develop a framework for the admission and evaluation of digital evidence that considers not only technical and legal aspects but is also aligned with Shariah values and principles. Such a framework will serve as a solid foundation for addressing cybercrime cases that fall within the jurisdiction of Islamic law.

In addition a sound and clearly defined investigative process is essential in Shariah criminal cases involving cyberspace. A well-structured investigation ensures that the evidence obtained is valid relevant and capable of being substantiated in court. This is vital in upholding the principle of justice while ensuring the effective enforcement of Shariah law during trial proceedings. A clear investigative process will ensure that all evidence gathered possesses a high probative value meaning that it can clearly and convincingly support the prosecution

or defence. With a structured procedure the risk of defects in the collection and presentation of evidence can be reduced thereby enhancing public confidence in the decisions of the court.

Moreover the rapid advancement of technology necessitates the reform of Shariah legal provisions to reflect the new realities involving the use of technology in the generation of evidence for prosecution purposes. The recognition of electronic evidence based on its appropriate probative value is a critical step in ensuring that the Shariah legal system remains relevant and effective. Amendments to Shariah law will clarify the process for the use of electronic evidence in court proceedings and thereby improve the overall effectiveness of the Shariah legal framework. In this regard the authors recommend the introduction of suitable standard operating procedures to govern the handling of Shariah criminal cases in cyberspace. These SOPs should cover investigation procedures the collection of electronic evidence and court procedures relevant to cyber-related Shariah offences. With clearly defined and comprehensive SOPs the Shariah judicial system will be able to function more efficiently and effectively in addressing cybercrime cases.

In conclusion these measures are expected to enhance the efficiency and effectiveness of the Shariah legal system in dealing with cyber offences. Through amendments that permit and expand the use of electronic evidence in a manner consistent with the Evidence Act 1950 and the implementation of structured SOPs the admission of electronic evidence can be undertaken with greater confidence which in turn will contribute to a more just and effective application of Islamic law.

ACKNOWLEDGMENT

The authors wish to express their gratitude to the Faculty of Law, University Kebangsaan Malaysia for funding this research through the Faculty Competitive Grant (UU-2024-018).

REFERENCES

1. Abd al-Mutalib Abd. Razak Hamdan. (2007). Al-da'wa wa ithbatiha fi al-fiqh al-jina'i al-Islami. al-Iskandariyyah: Dar al-Fikr al-Jaami'.
2. Abdul Rahman Mustafa. (1988). Prinsip-prinsip undang-undang keterangan Islam: Satu pendekatan perbandingan. Kuala Lumpur: Al Rahmaniah.
3. Ibnu Taimiyyah, Ahmad. (2001). Majmu'ah al-Fatawa (Cet. ke-2, Jil. 7). Al-Mansurah: Dar al-Wafa'.
4. Mahmud Saedon A. Othman. (2003). Undang-undang keterangan Islam. Kuala Lumpur: Dewan Bahasa dan Pustaka.
5. Mohamad Ismail Hj. Mohamad Yunus. (2006). Kedudukan bahan bukti (exhibit) electronic dan digital dalam keterangan: Masalah dan cabaran masa kini. Kuala Lumpur: The INSAF Publication.
6. Muhammad Fawwaz. (2008). Al-Wajiz fi al-Quds al-Tiyara al-Elektroniyyah. 'Amman: Dar al-Thaqafah.
7. Abd Latif Muda & Rosmawati Ali. (2000). Perbahasan kaedah-kaedah fiqh. Kuala Lumpur: Pustaka Salam Sdn Bhd.
8. Ibnu Qayyim. (1996). I'lam al-Muwaqqi'in 'an Rabb al-'Alamin (Jil. 1). Beirut: Dar al-Kutub al-'Ilmiyyah.
9. Sybil Sharpe. (n.d.). Electronically recorded evidence: A guide to the use of tape and video recordings in criminal and civil proceedings.
10. Mohamad Azhan Yahya, Hammad Mohamad Dahalan & Suhaizad Saifuddin. (2021). Analysis Proses Pengumpulan Keterangan Dokumen Elektronik dalam Kes Jenayah Syariah. Islamiyyat: International Journal of Islamic Studies, 43, 17–28.
11. Mohamad Azhan Yahya, Ahmad 'Azam Mohd Shariff & Mohd Abu Hassan Abdullah. (2017). Keterangan dokumen dalam bentuk digital di Mahkamah Syariah: Analysis berkaitan definisi serta kebolehterimaannya di sisi prinsip Syariah di Malaysia. Journal Hukum.
12. Mohd Kamel Mat Salleh, Adibah Bahori & Mohamad Azhan Yahya. (2021). Position of fatwa in the constitution: a legal analysis. Pertanika Journal of Social Science and Humanities, 29(4), 2171–2188.
13. Moriazi bin Muhammad v Ajmawati binti Atan. (n.d.). Journal Hukum, Jil. XX, Bhg. 1, 105–121.
14. Ramalinggam Rajamanickam, Nur Insyirah Mohamad Noh & Anita Harun. (2022). Kebolehterimaan

keterangan electronic di Malaysia. Journal Hukum.
15. Mohd Sabree Nasri & Ruzman Md Noor. (2020). Keterangan pendapat pakar sebagai kaedah pembuktian dalam kesalahan jenayah Syariah di alam siber. Journal Hukum.
16. Akta Keterangan 1950 (Akta 56).
17. Akta Keterangan Mahkamah Syariah (Wilayah-Wilayah Persekutuan) 1997.
18. Enakmen Keterangan Mahkamah Syariah (Negeri Selangor) 2003.
19. Enakmen Tatacara Jenayah Syariah (Negeri Selangor) 2003.
20. Kanun Prosedur Jenayah (Akta 593).
21. Faris Fuad. (2024, April 18). Bekas juruteknik tak mengaku buat hantaran jelik berkait kalimah Allah. Berita Harian. https://www.bharian.com.my
22. Informan 1. (2018, Julai 9). Peguam Syarie Perak serta Pulau Pinang.
23. Informan 2. (2018, Januari 29). Pegawai Penyiasat, Jabatan Agama Islam Selangor, Shah Alam, Selangor.
24. Informan 3. (2018, Mei 2). Penolong Penguatkuasa Agama, Jabatan Agama Islam Negeri Johor, Johor Bahru, Johor.
25. Informan 4. (2018, April 11). Peguam Syarie Negeri Selangor.
26. Ahmad Najib bin Aris v PP [2009] 2 MLJ 613.
27. Alliance dan Leicester Building v Ghahremani [1992] 142 NLJ 313.
28. Mohd Ali Jaafar v PP [1998] 4 MLJ.
29. Munah bte Ali v PP [1958] 1 MLJ 159.
30. Pendakwa Raya v Jawan Empaling [1996] 2 CLJ.
31. R. v Maqsud Ali [1965] 2 All ER 464.
32. R.M. Malkani v State of Maharashtra [1973] AIR 157.
33. Rama Reddy v V.V. Giri [1971] AIR 1162.
34. Taylor v Chief Constable of Cheshire [1987] 1 All ER 225.
35. Yusufali v State of Maharashtra [1967] 3 SCR 720.
36. Z.B. Bukhari v B.R. Mehra [1975] AIR 1778.