

Privacy, Security, and Ethics in Technology: A Qur'anic Perspective Through Cybercrime

Septi Aisyah^{1*}, Muhammad Farhan Bin Mat Noradin²

¹ Universitas Muhammadiyah Surakarta, Indonesia

² Selangor Islamic University, Malaysia

Article Info

Article History:

Received: 26 December 2024

Revised: 09 January 2025

Accepted: 28 February 2025

Published: 28 March 2025

*Corresponding Author:

Name: Septi Aisyah

Email:

g100231101@student.ums.ac.id

Keywords

Abstract

The rapid advancement of technology has significantly facilitated human activities, particularly in communication. However, technology is often misused for unethical and criminal purposes, such as theft, spreading misinformation, hate speech, and various forms of fraud. This study employs a literature research method with a maudhui approach based on Al-Farmawi's framework. The findings indicate that the Qur'an provides clear guidance on privacy, security, and ethical principles in the use of technology. These principles serve as a foundation for addressing contemporary issues, including cybercrime, from an Islamic perspective. The study underscores the relevance of Qur'anic values in mitigating the ethical dilemmas posed by technological advancements. For future research, it is recommended to explore the practical implementation of Qur'anic ethical principles in digital policies and cybersecurity frameworks. Additionally, empirical studies on the effectiveness of Islamic ethics in preventing cybercrimes, as well as comparative analyses between Qur'anic perspectives and modern cybersecurity regulations, could provide further insights into developing ethical and secure digital environments.

Privacy, Ethics in Technology, Cybercrime, Security

Abstrak

Kemajuan teknologi yang pesat telah secara signifikan mempermudah berbagai aktivitas manusia, terutama dalam komunikasi. Namun, teknologi sering disalahgunakan untuk tujuan yang tidak etis dan kriminal, seperti pencurian, penyebaran informasi yang salah, ujaran kebencian, serta berbagai bentuk penipuan. Penelitian ini menggunakan metode penelitian kepustakaan dengan pendekatan maudhui berdasarkan kerangka Al-Farmawi. Hasil penelitian menunjukkan bahwa Al-Qur'an memberikan panduan yang jelas mengenai privasi, keamanan, dan prinsip etika dalam penggunaan teknologi. Prinsip-prinsip ini menjadi dasar dalam menghadapi permasalahan kontemporer, termasuk kejahatan siber, dari perspektif Islam. Studi ini menegaskan relevansi nilai-nilai Qur'ani dalam mengatasi dilema etika yang muncul akibat kemajuan teknologi. Untuk penelitian selanjutnya, disarankan untuk mengeksplorasi implementasi praktis prinsip etika Qur'ani dalam kebijakan digital dan kerangka keamanan siber. Selain itu, studi empiris mengenai efektivitas etika Islam dalam mencegah kejahatan siber, serta analisis perbandingan antara perspektif Qur'ani dan regulasi keamanan siber modern, dapat memberikan wawasan lebih lanjut dalam pengembangan lingkungan digital yang etis dan aman.

Kata Kunci: Privasi, Etika dalam Teknologi, Kejahatan Dunia Maya, Keamanan

INTRODUCTION

The rapid advancement of information technology has transformed various aspects of human life, particularly in communication and social interaction. The internet has become an inseparable part of daily activities, enabling people to connect across vast distances instantly. In

Indonesia, the number of active social media users continues to rise significantly each year. In 2022, there was an increase of 12.35% compared to the previous year, reaching approximately 191 million users (Dawitri & Amara, 2023). This figure indicates that more than half of Indonesia's population actively engages in social media platforms. While technological progress has provided numerous benefits, it has also introduced various ethical and security challenges, including privacy breaches, cybercrimes, and the erosion of moral values in digital interactions (Hasan et al., 2024).

The widespread use of social media has altered social norms, particularly in Indonesia, a country known for its cultural values of politeness and hospitality. However, these values often seem neglected in cyberspace. A study conducted by Microsoft in 2021 ranked Indonesia 29th in the Digital Civility Index (DCI), with a score of 76, indicating a low level of online civility. This score is significantly lower than neighboring countries like Singapore and Taiwan. The decline in digital etiquette is evident in the increasing prevalence of hate speech, cyberbullying, online fraud, and the dissemination of misinformation. A quick glance at the comment sections of social media platforms such as Instagram, TikTok, and Twitter reveals an alarming amount of disrespectful and offensive language, reflecting a shift in online behavior that contradicts Indonesia's traditional values.

Cybercrime is one of the most pressing issues associated with the misuse of technology. The rise of digital transactions, coupled with economic uncertainties during the COVID-19 pandemic, has led to a surge in cybercrimes, including identity theft and financial fraud. Cases of unauthorized access to personal data, misuse of identity information for illegal online loans, and digital scams have become increasingly common. Victims often find themselves facing significant financial and legal repercussions due to stolen personal information. According to data from Surfshark, a Netherlands-based cybersecurity company, Indonesia ranked third globally in terms of data breaches, with 12.74 million accounts compromised in the third quarter of 2022 alone, surpassing even the United States and China, which have much larger populations.

While technology is designed to enhance human convenience and efficiency, its misuse for unethical and criminal purposes poses serious threats to digital security and ethical standards. Cybercrime does not emerge due to technology itself but rather from the irresponsible actions of individuals who exploit digital advancements for malicious purposes (Kraemer-Mbula et al., 2013). The ethical responsibility of using technology lies in human hands, and therefore, addressing cybercrime requires not only legal and technical solutions but also ethical guidance and moral accountability.

Most existing research on cybercrime has focused on legal frameworks and modern regulations aimed at preventing and punishing digital offenses. However, few studies have explored the ethical and moral dimensions of cybercrime from a religious perspective, particularly in relation to the Qur'anic teachings (Gesyani et al., 2023). One study that addresses this issue by Tanjung & Abdullah (2025). Their research highlights the ethical principles found in the Qur'an that guide online communication, emphasizing the importance of spreading peace (Salam), promoting goodness (Ma'ruf), and verifying information before sharing (Tabayyun). While this study focuses on general ethical behavior in social media, it does not comprehensively address various forms of cybercrime and their ethical implications in the Qur'anic context.

This study seeks to fill that gap by analyzing different types of cybercrimes, such as unauthorized access, illegal content distribution, digital fraud, and identity theft, through the lens of Qur'anic ethics. Although the Qur'an was revealed in a pre-digital era, its moral and ethical teachings remain relevant for contemporary challenges, including cybercrime. By examining Qur'anic principles related to privacy, security, and ethical conduct, this study aims to provide an alternative framework for addressing cybercrimes from an Islamic perspective.

Given the increasing complexity of cybercrime patterns and their impact on society, it is crucial to explore ethical solutions alongside legal and technical measures. This article contributes to the discussion by offering a Qur'anic perspective on cybercrime, emphasizing the importance of ethical responsibility in digital interactions. The findings of this study are expected to guide individuals, policymakers, and digital users in adhering to ethical principles derived from the Qur'an, fostering a safer and more responsible digital environment.

METHOD

This research is qualitative research conducted through library research that refers to information or textual resources about the subject under discussion. The approach in this study is the thematic approach according to Al-Farmawi, namely by gathering Qur'anic passages with similar meanings or discussing the same problem topic. After that, the verses are arranged according to chronology and the reason for the descent of the verse and give the information and explanations and draw conclusions. The resulting data is the answer to the problem statement.

Both data sources; primary and secondary data sources are used in this study. The primary source of data is the book "Tafsir Al-Misbah" by M. Quraish Shihab. Secondary data sources include library reference materials that support this research and books that complement the primary data above, such as the book of "Tafsir Ibn Kathir", the book of "Al-Qur'an dan Tafsirnya (Qur'an and its Tafsir)" by the Ministry of Religious Affairs of the Republic of Indonesia, the book "Kejahatan di Bidang Komputer" and various other references, books, and journals.

RESULTS AND DISCUSSION

Definition of Cybercrime According to Experts

Cybercrime is any criminal activity carried out using a computer, computer network or the internet. Cybercrime means using technology to commit bad deeds, illegal activities, target victims, or exploit vulnerabilities in digital systems. According to Andi Hamzah (1987), he defines cybercrime as: "Computer crime can be broadly understood as the unlawful use of computers." Susan W. Brenner (2011) in her article entitled "Defining Cybercrime: A Review of State and Federal Law" does not formulate a definition of cybercrime but describes it in 3 categories, i.e. crimes when: computers as targets of criminal activity, computers as tools or means of committing crimes, and computers as incidental aspects of evil acts.

A study from the United States Congress concluded that there are three categories of computer crimes: improper use of data into computers, altering or damaging information or archives, theft by electronics or other means (money, objects, facilities and valuable data) (Widyopramono, 1994). From a few of the previously mentioned understandings, cybercrime is

described as illegal activities conducted online, depending on computer expertise and telecommunications technology (Abidin & Sudirman, 2022).

Types of Cybercrime and Their Solutions According to the Qur'an

1. Unauthorized Access to Computer System and Service

The criminal act of illegally accessing or infiltrating a computer network system without authorization or knowledge of the system's owner constitutes. Unauthorized access tends to be a threat to a party's ownership. One step performs this action by probing or port scanning. Probing can be understood as the first step taken by the perpetrator before entering the victim's server by looking at what services and programs are available on the target server. The case in point is the hijacking of President SBY's (www.presidensby.info) website which displayed a black screen and the words "Hacked by MJL007! This is a PayBack from Jember Hacker Team".

In Islam, unauthorized access is reprehensible. This act if analogous to the real world is an act of entering someone else's house without permission. The perpetrator will see if the door of the target's house is locked, the type of lock used, what part is open and so on before launching the action.

يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْذِنُوا وَتُسَلِّمُوا عَلَىٰ أَهْلِهَا ذَٰلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُونَ

Means : “O you who have believed, do not enter houses other than your own houses until you ascertain welcome and greet their inhabitants. That is best for you; perhaps you will be reminded [i.e., advised]” (An-Nur [24] : 27)

This verse speaks of the ethics of visitation which is part of divine guidance related to human association. Al-Biqai'i connects this verse with past verses from the side that what the spreaders of the issue are in essence prejudice instilled by the devil in their hearts against the believers. In this verse Allah commands to close one of Satan's entrances by commanding Muslims to avoid places and causes that can arouse suspicion and prejudice. Therefore, here it is ordered to ask permission before entering the house.

Islam also stresses that when at the door, guests should not look straight at the door, let alone peer through the gap. This is another ethical point about asking permission. The left and right of the door is where it should be to avoid looking directly inside. In addition to emphasizing visiting ethics, in the context of cyberspace, its application can involve awareness not to violate the rights of others by illegally entering or infiltrating network systems (Shihab & Shihab, 2012).

2. Illegal Contents

Is entering data or information on something that is false, unethical, and may be seen as breaking the law or disrupting public order online. Examples include posting hoax or defamatory news that would degrade other people's dignity or self-worth, and posting pornographic content.

In the Qur'an there are several verses that regulate this. Including;

إِنَّ الَّذِينَ يُحِبُّونَ أَنْ تَشِيعَ الْفَاحِشَةُ فِي الَّذِينَ آمَنُوا لَهُمْ عَذَابٌ أَلِيمٌ فِي الدُّنْيَا وَالْآخِرَةِ وَاللَّهُ يَعْلَمُ وَأَنْتُمْ لَا تَعْلَمُونَ

Means : “Indeed, those who like that immorality should be spread [or publicized] among those who have believed will have a painful punishment in this world and the Hereafter. And Allah knows and you do not know.” (An-Nur [24] : 19)

In this verse Allah explains that those who like to broadcast such heinous and shameful acts as adultery among believers will be punished in this world and in the Hereafter. The dissemination of inappropriate news is forbidden in Islam. The preaching of adultery or pornography will have the devastating effect of encouraging people at large to commit adultery.

The word of (كَشَيْعٍ) means scattered. Al-Biqal'i derives the impression from the use of the word which is similar to the word Shi'a, that this verse hints at the pleasure of spreading abominations and that the absence of prevention against them can give birth to supporters of the abomination and followers of iniquity.

This verse can be used as a guide for those who are involved in the field of information. Here it reads their obligation to disseminate information that shouldn't be detrimental to society. In the book “Secercah Cahaya Ilahi (A glimmer of divine light)” The author suggests that both conveying good and positive information -as long as it is not excessive- so that it leads to praise that plunges, Medium negative ones are recommended not to be put forward except within the necessary limits. We don't need to 'strip' someone to prove their crime. We are also prohibited from informing of crimes/improprieties that may stimulate new crimes. Nor does it reveal people's feuds, thus further aggravating the situation (Shihab & Shihab, 2012).

A similar verse leads Muslims by reminding them that Allah the Most Holy does not like blatant acts of ugliness concerning anything.

لَا يُحِبُّ اللَّهُ الْجَهْرَ بِالسُّوِّءِ مِنَ الْقَوْلِ إِلَّا مَنْ ظَلِمَ ۗ وَكَانَ اللَّهُ سَمِيعًا عَلِيمًا

Means : “Allah does not like the public mention of evil except by one who has been wronged. And ever is Allah Hearing and Knowing.” An-Nisa' [4] : 148)

God does not like His servants who speak bad words to anyone. Bad words can cause hostility and hatred among members of society. If this happens for a long time it can lead to denial of rights and bloodshed, and can also influence those who hear it to imitate the act (Amirotussolihah dkk., 2022). In this verse there is an exception for the persecuted person (victim). He is allowed and even obliged to complain the person who persecuted him to a judge or the authorities who can provide assistance in eliminating tyranny (Ramanda, 2024).

3. Data Forgery

Forging information on crucial documents that are online kept and then make the data as if there was a typo so that the perpetrator can benefit from the document error is illegal. For example, falsifying a bank's website. The perpetrator will spread the fake bank website link and when the target makes a transaction through the link, the account number and pin will be known to the perpetrator (Sari dkk., 2024).

With regard to falsifying documents, God has warned people not to cheat and harm people.

وَلَا تَلْبِسُوا الْحَقَّ بِالْبَاطِلِ وَتَكْتُمُوا الْحَقَّ وَأَنْتُمْ تَعْلَمُونَ

Means : “And do not mix the truth with falsehood or conceal the truth while you know [it].” (Al-Baqarah [2] : 42)

In this verse there are two kinds of Allah's prohibitions directed at the Children of Israel, namely the prohibition against mixing the right with the vanity, polish the vanity with the right, hide the right, and reveal the vanity and do not hide the truth, even though they know it.

It may also be interpreted as 'while you know (it / consequences of these actions)', which is to have a great effect on mankind. The great harm is that they go astray from the path of guidance that plunges them into hell if they take the path of immorality that you have shown them, but you polish with a kind of thing that is right in order to be accepted by them. And also you color it with explanations and captions. Vice versa, namely hiding the right and mixing it with the vanity (*Al-Qur'an dan tafsirnya*, 2010).

4. Cyber Bullying

It is bullying or bullying carried out online through the internet and other technologies. For example, spreading lies about someone, posting embarrassing photos of others, sending threatening messages through chat platforms and ostracizing or insulting in the comments (Giumetti & Kowalski, 2022).

يَا أَيُّهَا الَّذِينَ آمَنُوا لَا يَسْخَرْ قَوْمٌ مِّن قَوْمٍ عَسَىٰ أَن يَكُونُوا خَيْرًا مِّنْهُمْ وَلَا نِسَاءٌ مِّن نِّسَاءٍ عَسَىٰ أَن يَكُنَّ خَيْرًا مِّنْهُنَّ وَلَا تَلْمِزُوا أَنفُسَكُمْ وَلَا تَنَابَرُوا بِالْألقَابِ بِئْسَ الإِسْمُ المُسْوُوقُ بَعْدَ الإِيمَانِ وَمَن لَّمْ يَتُبْ فَأُولَئِكَ هُم الظَّالِمُونَ

Means: “O you who have believed, let not a people ridicule [another] people; perhaps they may be better than them; nor let women ridicule [other] women; perhaps they may be better than them. And do not insult one another and do not call each other by [offensive] nicknames. Wretched is the name [i.e., mention] of disobedience after [one's] faith. And whoever does not repent – then it is those who are the wrongdoers.” (Al-Hujurat [49] : 11)

The above verse gives instructions on some things to avoid to prevent bullying, namely making fun of each other (يَسْخَرُ) , mocking (تَلْمِزُوا) , and summoned with a title judged poorly by the summoned (تَنَابَرُوا بِالْألقَابِ). Word (يَسْخَرُ) / making fun is mentioning the shortcomings of the other party in an attempt to make fun of the person concerned, either through actions, words, or conduct. The use of the word *qaumun* indicates a group of men only because the verse above also mentions women specifically. The mention of the word *nisa'* (women) separately aims to emphasize the verse, as mocking and gossiping are more common among women than among men.

Scholars differ in the meaning of the word (تَلْمِزُوا). According to Ibn Assyria the word means ridicule that is directly confronted by the ridiculed, either by gestures, lips, hands, or words understood as ridicule or threat. The word of (تَنَابَرُوا) taken from the word (النَّبذ) that mean bad title. *At-tanabuz/tanabazu* is giving each other bad titles. Don't use word forms that contain reciprocal meanings unlike *al-lamzu's* (تَلْمِزُوا) prohibition in the previous passage. This is because bad titles are usually conveyed blatantly by calling the person concerned. This invites anyone offended by the bad call to reply with a similar call so that *tanabuz* occurs (Wati, 2022).

5. Cyber Sabotage and Extortion

Is an illegal by interfering with, destroying, or causing harm to any data, software, or computer network system that is connected to the internet. For example, infiltrating a virus into a computer program system so that it does not run as it should (Hapsah & Nasution, 2023). The act of infiltrating viruses into the computer is considered as an act of damaging, disturbing and harming other parties.

وَلَا تَبْخَسُوا النَّاسَ أَشْيَاءَهُمْ وَلَا تَعْتُوا فِي الْأَرْضِ مُفْسِدِينَ

Means : “And do not deprive people of their due and do not commit abuse on earth, spreading corruption.” (Ash-Shu'ara [26] : 183)

M. Quraish Shihab in his book Tafsir Al-Misbah (Shihab & Shihab, 2012) mentioned the meaning of the word (تَعْتُوا) is destruction or haste to do so. That is, do not do damage deliberately. This verse is a prohibition against destruction and various crimes of any kind both murder, adultery, violation of rights and both material and immaterial, and so on. Basically, the principle of human relations according to Islam is that it should not be tyrannical and should not be persecuted in any way and in any field (Al-Hamid, 2022).

6. Offense against Intellectual Property

That is a crime committed online that targets the intellectual property rights of other people. The example is illegal distribution of other people's works such as books in the form of soft files. Taking other's work without authorization is an act that does not respect the work of others, even not in accordance with religious norms. In Islam, taking someone else's work (plagiarism) and even spreading and profiting by selling it is equivalent to eating someone else's property and the law is haram (Pratama, 2020).

وَلَا تَأْكُلُوا أَمْوَالَكُمْ بَيْنَكُمْ بِالْبَاطِلِ وَتُدْلُوا بِهَا إِلَى الْحُكَّامِ لِتَأْكُلُوا فَرِيقًا مِّنْ أَمْوَالِ النَّاسِ بِالْإِثْمِ وَأَنْتُمْ تَعْلَمُونَ

Means : “And do not consume one another's wealth unjustly or send it [in bribery] to the rulers in order that [they might aid] you [to] consume a portion of the wealth of the people in sin, while you know [it is unlawful].” (Al-Baqarah [2] : 188)

In Tafsir Jalalain it is explained, 'and do not eat the property among you in a vanity way' means the path that is haram according to the Shari'a, either by stealing, intimidating and others. As for the tafsir Al-Misbah means violation of the provisions of religion and sharia.

In this context, plagiarism is an act of violating sharia because it does not respect the efforts of others by eating people's property without permission. Eating property here is not only interpreted as a form of ownership of objects or goods, but includes all aspects of life including intellectual property (Setyaningias & Atika, 2023).

7. Infringements of Privacy

Or invasion of privacy is a crime committed against someone's very private and personal information. This crime typically targets a person's personal information that is kept on a computerized personal data form and that, if discovered by others, could cause the victim material

or immaterial harm. Examples of this type of information include credit card numbers, ATM PIN numbers, concealed illnesses or defects, and so forth. For example, the Tokopedia data leak in May 2020. This data was then sold by hackers who according to @underthhbreach twitter account sold for 5,000 USD (Yulianti, 2021).

In Islam, privacy is respected as an individual right. Islam stresses the importance of safeguarding the honor and rights of every individual. In connection with the case above, perpetrators of privacy violations are considered as acts of stealing, whether the perpetrators use privacy and target data for sale or for other benefits.

وَالسَّارِقُ وَالسَّارِقَةُ فَاقْطَعُوا أَيْدِيَهُمَا جِزَاءً بِمَا كَسَبَا نَكَالًا مِّنَ اللَّهِ يَوْمَ اللَّهُ عَزِيزٌ حَكِيمٌ

Means : “[As for] the thief, the male and the female, amputate their hands in recompense for what they earned [i.e., committed] as a deterrent [punishment] from Allah. And Allah is Exalted in Might and Wise.” (Al-Ma'idah [5] : 38)

Cases that are also classified as types of privacy violations are cyber stalking or cyber stalking. Cyber stalking is a crime committed by spying on the target and then stealing all his information to disrupt or harass by utilizing internet media. Some of the usual motives include making false accusations about targets online, making death threats or publishing personal information (Zaki, 2022).

يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِّنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ وَلَا تَجَسَّسُوا وَلَا يَغْتَبَ بَعْضُكُم بَعْضًا أَيُحِبُّ أَحَدُكُمْ أَنْ يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ وَاتَّقُوا اللَّهَ إِنَّ اللَّهَ تَوَّابٌ رَّحِيمٌ

Means : “O you who have believed, avoid much [negative] assumption. Indeed, some assumption is sin. And do not spy or backbite each other. Would one of you like to eat the flesh of his brother when dead? You would detest it. And fear Allah; indeed, Allah is Accepting of Repentance and Merciful.” (Al-Hujurat [49] : 12)

This verse is still a continuation of the guidance of the previous verse. It's just that the bad things in this verse are hidden. Three hidden bad things are forbidden by Allah in this verse, namely prejudice, spying or trying to find out the faults of others and ghibah (backbiting). The sentence of (اجْتَنِبُوا كَثِيرًا مِّنَ الظَّنِّ) affirming that some conjectures are sinful that was unfounded conjectures. Usually an unfounded conjecture that results in sin is a bad accusation against the other party. This means that the above verse forbids making bad accusations without basis because it can plunge a person into sin.

The word of (تَجَسَّسُوا) is an effort to learn information covertly (spy). Finding fault with others is usually born of negative allegations against him, therefore he is mentioned after the prohibition of conjecture. The term of (يَغْتَابُ) is the root from the word (غَيْبٌ) which means calling another person who absent from in front of the denominator with anything the individual dislikes even though the ugliness revealed is indeed carried by the object of grant, it is forbidden. If the so-called evil is not carried by the person concerned, then it is called a big lie (Sholihah, 2024).

Based on the description above regarding observations of various forms / types of cybercrime that occur, it can be concluded that cybercrime includes traditional crimes that use

information and communication technology as a tool or media and new crimes that can only occur in cyberspace.

CONCLUSION

Cybercrime is an evolving form of crime that continues to grow alongside advancements in information technology, encompassing various illegal activities that utilize computers, networks, or the internet as tools or targets of criminal acts. Common types of cybercrime include unauthorized access to computer systems, the distribution of illegal content, data forgery, and cyberbullying. From an Islamic perspective, these actions contradict the moral and ethical principles taught in the Qur'an, such as honesty, justice, and respect for individual rights. Therefore, Islam encourages its followers to refrain from all forms of digital crimes and to cultivate awareness of responsible technology use.

Although this study provides insights into cybercrime from an Islamic perspective, several limitations must be acknowledged. This research primarily focuses on conceptual and normative aspects without an empirical analysis of cybercrime cases within Muslim communities. Additionally, it does not extensively discuss prevention strategies or legal policies implemented in various Muslim countries. Future studies are encouraged to conduct empirical research on cybercrime trends and the effectiveness of legal policies in combating these crimes. Furthermore, developing digital education strategies based on Islamic values is crucial for raising public awareness of cyber threats and fostering a safe and ethical digital environment.

REFERENCES

- Abidin, D. Z., & Sudirman, J. J. (2022). *Kejahatan Dalam Teknologi Informasi Dan Komunikasi*.
- Al-Hamid, M. S. (2022). Illicit Enrichment Dalam Upaya Pemberantasan Korupsi Di Indonesia. *Al-Mizan*, 18(2), 243–268. <https://doi.org/10.30603/am.v18i2.2900>
- Al-Qur'an dan tafsirnya* (Ed. yang disempurnakan). (2010). Lentera Abadi.
- Amirotussolihah, A., Muslihah, S. F., Ismatulloh, A. M., & Rozi, A. F. (2022). Larangan Hate Comment di Media Sosial Kontekstualisasi Q.S. An-Nisa': 148 (Tinjauan Analisis Ma'na-Cum-Maghza). *Islamika: Jurnal Ilmu-Ilmu Keislaman*, 22(01), 114–129. <https://doi.org/10.32939/islamika.v22i01.1143>
- Dawitri, N., & Amara, M. (2023). *Indonesia's Low Digital Civility Index -Two Sides of Indonesia*. <https://doi.org/10.13140/RG.2.2.17889.58721>
- Giumetti, G. W., & Kowalski, R. M. (2022). Cyberbullying via social media and well-being. *Current Opinion in Psychology*, 45, 101314. <https://doi.org/10.1016/j.copsyc.2022.101314>
- Gesyani, H., Ritonga, A. W., Arab, I., & Ningsih, I. (2023). Budaya Pendidikan Al-Qur'an Bagi Anak Usia Dini di Era Teknologi. *Awladuna: Jurnal Pendidikan Islam Anak Usia Dini*, 1(2), 16–27. <https://doi.org/10.61159/awladuna.v1i2.116>
- Hapsah, Z. F., & Nasution, M. I. P. (2023). *Analisis Tingkat Keamanan Data Perusahaan yang Rentan Terhadap Serangan Cyber Dalam Sistem Informasi Manajemen*. 1(2). <https://doi.org/10.62017/wanargi>
- Hasan, K., Abdullah, & Ahyar. (2024). Islamic Communication Ethics: Concepts and Applications In The Digital Era. *Jurnal Al-Fikrah*, 8523, 97–111.

- <https://doi.org/https://doi.org/10.54621/jiaf.v13i1.734>
- Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The Cybercrime Ecosystem: Online Innovation in the Shadows? *Technological Forecasting and Social Change*, 80(3), 541–555. <https://doi.org/10.1016/j.techfore.2012.07.002>
- Pratama, F. C. B. (2020). Legal Protection of Intellectual Property Rights for Copyright Holders in the Perspective of Community Legal Culture. *Journal of Creativity Student*, 5(1), 1–24. <https://doi.org/10.15294/jcs.v5i1.36277>
- Ramanda, B. Z. (2024). *Makna Surah An-Nisa' Ayat 148 Dalam Al-Qur'an Perspektif Tafsir Al-Azhar Karya Buya Haji Abdul Malik Karim Amrullah*. 1.
- Sari, H. P., Mulyani, D. I., Nilamsari, M. A., Sitorus, D. D. F., & Harimurti, Y. W. (2024). *Efektivitas Hukum Perlindungan Data Pribadi Terhadap Kejahatan Siber Di Indonesia*.
- Setyaningtias, P., & Atika, A. (2023). Penyebaran Spoiler di Media Tiktok Terhadap Film Spiderman: No Way Home Perspektif Hukum Pidana Islam. *Ta'zir: Jurnal Hukum Pidana*, 7(1), 1–21. <https://doi.org/10.19109/tazir.v7i1.17714>
- Shihab, M. Q., & Shihab, M. Q. (2012). *Surah al-Furqân, Surah asy-Syu'arâ', Surah an-Naml, Surah al-Qashash* (Cetakan V). Lentera Haiti.
- Sholihah, I. M. (2024). *Batasan Prasangka Buruk Perspektif M. Quraish Shihab Dalam Tafsir Al-Misbab Surat Al-Hujurat Ayat 12*.
- Tanjung, M. T. H., & Abdullah, A. (2025). The Concept of Communication in the Quran; Analysis of Theory and Practice. *International Journal Of Education, Social Studies, And Management (IJESSM)*, 5(1), 72–85. <https://doi.org/10.52121/ijessm.v5i1.629>
- Wati, R. (2022). *Nilai-Nilai Pendidikan Akhlak Dalam Al-Qur'an Surat Al-Hujurat Ayat 11-13 (Perbandingan Tafsir Ibnu Katsir Dan Tafsir Al-Misbab)*.
- Widyopramono. (1994). *Kejahatan di bidang komputer* (Cet. 1). Pustaka Sinar Harapan.
- Yulianti, F. (2021). *Contoh Kasus Cyber Crime Dan Penyelesaiannya* [UNIKOM]. <http://repository.unikom.ac.id/id/eprint/68705>
- Zaki, M. M. (2022). Aspek Pidana Cyberstalking Sebagai Salah Satu Bentuk Cybercrime. *Jurist-Diction*, 5(3), 973–988. <https://doi.org/10.20473/jd.v5i3.35790>