Journal of Law and Administrative Science (JLAS)
**Volume 3 Nomor 2 Oktober 2025**
e-ISSN :2988-103X; p-ISSN :2988-1048, Hal 50-75
DOI: 10.33478/jlas.v3i2.45

# BUILDING TRUST IN THE DIGITAL WORLD: STRENGTHENING CYBER REGULATIONS, ADDRESSING THE CHALLENGES OF SURVEILLANCE TECHNOLOGY FROM AN ISLAMIC PERSPECTIVE

**Wahyu Fahmi Rizaldy[1*], Justino Ximenes Sopalo [2]**

[1]Universitas Teknologi Surabaya, Indonesia
[2]Universitas Dili, Timor Leste
*Wahyufahmi3112@gmail.com

Alamat: Jalan Balongsari Praja V No.1 Tandes, Surabaya
*Korespondensi penulis: wahyufahmi3112@gmail.com*

***Abstract***. *The digital era has significantly transformed human interaction, presenting complex opportunities and challenges. Trust is a crucial pillar in building healthy and productive interactions in the digital world. However, this trust is threatened by various factors, including cybercrime, the spread of misinformation, and increasingly invasive surveillance technology. In this context, the Islamic perspective offers a comprehensive ethical framework for building trust in the digital age. This research aims to explore how Islamic principles can be applied to build trust in the digital world. The study will identify Islamic principles relevant to building trust, develop a cyber regulation framework based on Islamic values, and formulate strategies to address the challenges of surveillance technology while considering Islamic ethics and values. A normative legal approach will be employed, focusing on regulatory studies, analysis of primary and secondary Islamic legal sources, and a comparative study of cyber regulations in Muslim-majority countries. This research is expected to make a significant contribution to formulating effective, ethical, and equitable cyber regulations, as well as addressing the challenges of surveillance technology in the digital age.*

***Keywords***: *Trust, Digital World, Cyber Regulation, Surveillance Technology, Islamic Perspectiveyouyoutbe*

**Abstrak**. Era digital telah mengubah cara interaksi manusia secara signifikan, menghadirkan peluang dan tantangan yang kompleks. Kepercayaan menjadi pilar penting dalam membangun interaksi yang sehat dan produktif di dunia digital. Namun, kepercayaan ini terancam oleh berbagai faktor, termasuk kejahatan siber, penyebaran hoaks, dan teknologi pengawasan yang semakin invasif. Dalam konteks ini, perspektif Islam menawarkan kerangka etis yang komprehensif untuk membangun kepercayaan di era digital. Penelitian ini bertujuan untuk mengeksplorasi bagaimana prinsip-prinsip Islam dapat diterapkan dalam membangun kepercayaan di dunia digital. Penelitian ini akan mengidentifikasi prinsip-prinsip Islam yang relevan dalam membangun kepercayaan, mengembangkan kerangka kerja regulasi siber yang berbasis pada nilai-nilai Islam, dan merumuskan strategi untuk menghadapi tantangan teknologi pengawasan dengan mempertimbangkan etika dan nilai-nilai Islam. Pendekatan hukum normatif akan digunakan dengan fokus pada studi regulasi, analisis sumber-sumber hukum Islam primer dan sekunder, serta studi komparatif terhadap regulasi siber di negara-negara dengan mayoritas Muslim. Penelitian ini diharapkan dapat memberikan kontribusi yang signifikan dalam merumuskan regulasi siber yang efektif, etis, dan berkeadilan, serta dalam menghadapi tantangan teknologi pengawasan di era digital.

**Kata kunci**: Kepercayaan, Dunia Digital, Regulasi Siber, Teknologi Pengawasan, Perspektif Islam.

*Received: Septermber 29, 2024; Revised: Oktober 20, 2025; Accepted: Oktober 30, 2025*
*Corresponding author, wahyufahmi3112@gmail.com

## 1. INTRODUCTION

The digital age has fundamentally transformed the landscape of human interaction, presenting unprecedented opportunities and challenges. On one hand, digital technology has opened up access to information, facilitated communication, and driven innovation in various fields. On the other hand, this technological advancement has also given rise to the potential for serious misuse, such as cybercrime, the spread of fake news, and privacy violations. A global survey by DataProt in 2023 revealed that 64% of internet users are concerned about the security of their personal data.(DataProt, 2023) Additionally, the 2023 We Are Social report revealed that Indonesia ranks 6th globally in the number of malware attacks.(We Are Social Digital, 2023)

This situation is further exacerbated by the rapid development of increasingly sophisticated and invasive surveillance technologies. Surveillance cameras with facial recognition, location tracking through mobile phones, and online activity monitoring have become part of everyday life.(Ananda, 2023) Although this technology has the potential to benefit security and order, its uncontrolled use can threaten human rights and individual freedoms.

In facing the complexities of the digital world, trust becomes a crucial element that must be built and maintained. Without trust, online interactions and transactions will be hindered, innovation will be stifled, and society will be fragmented. Therefore, strong and ethical cyber regulations are needed to protect user rights, prevent technology misuse, and build a safe and trustworthy digital environment.(Putra, 2023)

In this context, the Islamic perspective can provide a significant contribution. Islam possesses a set of universal values and moral principles, such as honesty, justice, and respect for human rights. These values can serve as an ethical foundation for designing effective and equitable cyber regulations, as well as for addressing the increasingly complex challenges of surveillance technology.

Furthermore, Islamic teachings on safeguarding privacy and individual dignity can guide the formulation of personal data protection policies in the cyber realm. Islam also emphasizes the importance of balance between openness and control, between freedom of expression and social responsibility. These principles are

relevant in navigating ethical dilemmas related to the use of surveillance technology, such as social media monitoring or the use of artificial intelligence in decision-making.(Angriani, 2021) Thus, the Islamic perspective can provide a comprehensive ethical framework to address the challenges of surveillance technology in this digital age. This research aims to explore how Islamic principles can be applied to build trust in the digital world. Specifically, this research will identify Islamic principles relevant to building trust, develop a cyber regulation framework based on Islamic values, and formulate strategies to address surveillance technology challenges while considering Islamic ethics and values.

To achieve these objectives, this research will utilize a normative legal approach with a focus on regulatory studies. An in-depth analysis will be conducted on primary sources of Islamic law such as the Quran and Hadith, as well as secondary sources such as fiqh books and scholarly opinions. Additionally, this research will examine relevant cyber regulations at both national and international levels to identify alignment and potential conflicts with Islamic principles. A comparative study of cyber regulations in Muslim-majority countries will also be conducted to enrich the analysis and provide more comprehensive recommendations.

## 2. THEORETICAL REVIEW

In addressing the challenges and opportunities of the digital world, Islam offers relevant moral and ethical principles for formulating effective and equitable cyber regulations. These principles are rooted in fundamental Islamic values, such as justice, public interest, respect for human dignity, and social responsibility.

Islam highly upholds the right to individual privacy. In the Qur'an, Allah SWT states, "And do not spy or backbite each other." (QS. Al-Hujurat: 12). This verse emphasizes the importance of maintaining privacy and avoiding actions that could harm others. In the digital context, this principle translates to the protection of users' personal data, including identity information, preferences, and online activities.(Wahyuningati & Utami, 2023) Islamic cyber regulations must ensure that personal data is only collected and used with user consent, and is protected from unauthorized access and misuse.

Islam teaches the importance of maintaining security and order in society. This principle also applies in cyberspace, where information security is crucial. Islamic

cyber regulations should include measures to protect systems and networks from cyber attacks, such as hacking, data theft, and malware distribution.(M. Syafii Maarif, 2022) Furthermore, it is crucial to provide legal protection for victims of cybercrimes, such as online fraud and defamation. This effort aligns with Islamic teachings on justice and the protection of individual rights.

Islam emphasizes the importance of transparency and accountability in every action. In a hadith, Prophet Muhammad (PBUH) said, "Whoever betrays a trust, then he does not belong to my group." This hadith emphasizes the importance of maintaining trust and being responsible for every action taken.(Waluya & Mulauddin, 2021) In the context of cyber regulation, this principle means that the use of technology must be done transparently and accountably. Governments, companies, and individuals must be responsible for their use of technology.

Transparency and accountability in cyber regulation also mean effective oversight of technology use, both by the government and the private sector. This oversight must be conducted independently and impartially, involving various stakeholders.(Rosidah et al., 2023) Furthermore, it is crucial to have accessible and effective complaint mechanisms, allowing the public to report violations or misuse of technology. Thus, the principles of transparency and accountability in Islam can serve as a strong foundation for establishing cyber regulations that are fair, responsible, and protect individual rights.

Islam prohibits the dissemination of harmful content, such as hate speech, slander, and pornography. These types of content can damage morality, cause conflict, and harm individuals and society. Islamic cyber regulations must prohibit the distribution of such content and impose strict sanctions on violators.(Almujaddedi & Hayati, 2022)

Furthermore, Islam encourages the use of digital technology for positive purposes, such as education, religious propagation (da'wah), and community development. Islamic cyber regulations should not only focus on prohibiting negative content but also encourage the production and dissemination of content that benefits humanity. In this way, digital technology can become a means to spread values of goodness and improve the quality of life for society.

Islam encourages the use of technology for the common good and the well-being of society. Technology can be used to improve the quality of education, healthcare, the economy, and various other aspects of life.(Suprapto & Yulianto, 2023) Islamic cyber regulation should promote the positive and productive use of technology, while restricting its use for harmful or destructive purposes.

In this regard, cyber regulations based on Islamic values can encourage technological innovation that benefits the wider community, such as the development of inclusive online education platforms, affordable healthcare applications, or fair Islamic financial systems. Additionally, these regulations can restrict the use of technology for negative purposes such as the spread of hoaxes, hate speech, or the exploitation of personal data. Therefore, Islamic cyber regulation not only governs the use of technology but also directs it to create a positive impact on human life and the environment.

These Islamic cyber regulation principles can be implemented in various ways. Firstly, the government needs to develop comprehensive laws and regulations to govern the use of digital technology. These laws should include privacy protection, prohibition of harmful content, and promotion of technology use for the common good.(Anggen Suari & Sarjana, 2023) In addition to regulation, it is also important to strengthen digital literacy in society. Education and training programs on responsible technology use, digital ethics, and cybersecurity need to be enhanced. With a more aware and skilled society in using technology, the negative potential of digital technology can be minimized.

Secondly, the government needs to establish an independent and effective supervisory body to oversee the implementation of cyber regulations. This body should have the authority to investigate violations, impose sanctions, and ensure that all parties comply with applicable regulations. The supervisory body also needs to have the ability to adapt quickly to the ever-changing developments in technology and cybercrime trends.(Khansa, 2021) Collaboration with experts, researchers, and international institutions in the field of cybersecurity is also crucial to ensure that regulations and law enforcement remain relevant and effective. Transparency and accountability in the operations of the supervisory body must also be maintained to build public trust and ensure that the power granted is not misused.

Thirdly, the government and relevant institutions need to educate the public about digital ethics and responsible technology use. This education is crucial to raise public awareness about their digital rights, the risks of technology misuse, and the importance of using technology ethically and responsibly.(Syafuddin et al., 2023) In addition to education, there should also be efforts to encourage public participation in the formulation of policies and regulations related to surveillance technology. Public involvement in this process will ensure that the resulting policies are not only effective but also reflect the values and interests of the community. Public participation can also enhance transparency and accountability in the use of surveillance technology, thereby minimizing the potential for misuse.

## 3. RESEARCH METHOD

This study utilizes a normative legal research (juridical-normative) method (Marzuki, 2014), also known as doctrinal research, which focuses on the analysis of legal rules, principles, and concepts related to cyber regulation and surveillance technology. The study employs a statute approach to systematically examine the hierarchy and substance of existing cyber regulations (such as the ITE Law and the PDP Law), and a conceptual approach to understand the essential meanings of digital trust, privacy, and surveillance. Specifically, this research also applies an Islamic law approach, using the Al-Qur'an, Hadith, and fiqh rules (particularly Qawa'id Fiqhiyyah) as primary norms to analyze ethical issues and the limitations of surveillance technology. Data collection is conducted through library research, relying on primary legal materials (statutes, regulations, and sacred texts) and secondary legal materials (scholarly journals, books, dissertations, and fatwas from scholars related to cyber Fiqh).

All collected data will be analyzed using qualitative analysis with legal interpretation methods, specifically systematic and teleological (sociological) interpretation. The data analysis does not aim to test hypotheses, but rather to construct a coherent legal argument. The analysis process involves identifying positive legal norms and Shari'a norms related to privacy (hifzhu al-'irdh), then comparing them with the challenges posed by surveillance technology. The results of

this analysis will be presented descriptively and prescriptively; that is, describing existing normative voids or conflicts, while also providing prescriptive recommendations for a cyber-regulation-strengthening model that is not only technically effective but also aligned with the principles of ethics and justice from an Islamic perspective.

## 4. RESULT AND DISCUSSION

## CYBER REGULATION IN ISLAMIC PERSPECTIVE

In addressing the challenges and opportunities of the digital world, Islam offers relevant moral and ethical principles for formulating effective and equitable cyber regulations. These principles are rooted in fundamental Islamic values, such as justice, public interest, respect for human dignity, and social responsibility.

### 1. Islamic Principles for Cyber Regulation

a. Privacy and Personal Data Protection:

Islam highly upholds the right to individual privacy. In the Qur'an, Allah SWT states, "And do not spy or backbite each other." (QS. Al-Hujurat: 12). This verse emphasizes the importance of maintaining privacy and avoiding actions that could harm others. In the digital context, this principle translates to the protection of users' personal data, including identity information, preferences, and online activities.(Wahyuningati & Utami, 2023) Islamic cyber regulations must ensure that personal data is only collected and used with user consent, and is protected from unauthorized access and misuse.

Islam teaches the importance of maintaining security and order in society. This principle also applies in cyberspace, where information security is crucial. Islamic cyber regulations should include measures to protect systems and networks from cyber attacks, such as hacking, data theft, and malware distribution.(M. Syafii Maarif, 2022) Furthermore, it is crucial to provide legal protection for victims of cybercrimes, such as online fraud and defamation. This effort aligns with Islamic teachings on justice and the protection of individual rights.

b. Transparency and Accountability:

Islam emphasizes the importance of transparency and accountability in every action. In a hadith, Prophet Muhammad (PBUH) said, "Whoever betrays a trust, then he does not belong to my group." This hadith emphasizes the importance of maintaining trust and being responsible for every action taken.(Waluya & Mulauddin, 2021) In the context of cyber regulation, this principle means that the use of technology must be done transparently and accountably. Governments, companies, and individuals must be responsible for their use of technology.

Transparency and accountability in cyber regulation also mean effective oversight of technology use, both by the government and the private sector. This oversight must be conducted independently and impartially, involving various stakeholders.(Rosidah et al., 2023) Furthermore, it is crucial to have accessible and effective complaint mechanisms, allowing the public to report violations or misuse of technology. Thus, the principles of transparency and accountability in Islam can serve as a strong foundation for establishing cyber regulations that are fair, responsible, and protect individual rights.

c. Prohibition of Harmful Content:

Islam prohibits the dissemination of harmful content, such as hate speech, slander, and pornography. These types of content can damage morality, cause conflict, and harm individuals and society. Islamic cyber regulations must prohibit the distribution of such content and impose strict sanctions on violators.(Almujaddedi & Hayati, 2022)

Furthermore, Islam encourages the use of digital technology for positive purposes, such as education, religious propagation (da'wah), and community development. Islamic cyber regulations should not only focus on prohibiting negative content but also encourage the production and dissemination of content that benefits humanity. In this way, digital technology can become a means to spread values of goodness and improve the quality of life for society.

d. Promotion of Technology Use for Public Good:

Islam encourages the use of technology for the common good and the well-being of society. Technology can be used to improve the quality of education, healthcare, the economy, and various other aspects of life.(Suprapto & Yulianto,

2023) Islamic cyber regulation should promote the positive and productive use of technology, while restricting its use for harmful or destructive purposes.

In this regard, cyber regulations based on Islamic values can encourage technological innovation that benefits the wider community, such as the development of inclusive online education platforms, affordable healthcare applications, or fair Islamic financial systems. Additionally, these regulations can restrict the use of technology for negative purposes such as the spread of hoaxes, hate speech, or the exploitation of personal data. Therefore, Islamic cyber regulation not only governs the use of technology but also directs it to create a positive impact on human life and the environment.

**2. Implementation of Islamic Cyber Regulation**

These Islamic cyber regulation principles can be implemented in various ways. Firstly, the government needs to develop comprehensive laws and regulations to govern the use of digital technology. These laws should include privacy protection, prohibition of harmful content, and promotion of technology use for the common good.(Anggen Suari & Sarjana, 2023) In addition to regulation, it is also important to strengthen digital literacy in society. Education and training programs on responsible technology use, digital ethics, and cybersecurity need to be enhanced. With a more aware and skilled society in using technology, the negative potential of digital technology can be minimized.

Secondly, the government needs to establish an independent and effective supervisory body to oversee the implementation of cyber regulations. This body should have the authority to investigate violations, impose sanctions, and ensure that all parties comply with applicable regulations. The supervisory body also needs to have the ability to adapt quickly to the ever-changing developments in technology and cybercrime trends.(Khansa, 2021) Collaboration with experts, researchers, and international institutions in the field of cybersecurity is also crucial to ensure that regulations and law enforcement remain relevant and effective. Transparency and accountability in the operations of the supervisory body must also be maintained to build public trust and ensure that the power granted is not misused.

Thirdly, the government and relevant institutions need to educate the public about digital ethics and responsible technology use. This education is crucial to raise public awareness about their digital rights, the risks of technology misuse, and the importance of using technology ethically and responsibly.(Syafuddin et al., 2023) In addition to education, there should also be efforts to encourage public participation in the formulation of policies and regulations related to surveillance technology. Public involvement in this process will ensure that the resulting policies are not only effective but also reflect the values and interests of the community. Public participation can also enhance transparency and accountability in the use of surveillance technology, thereby minimizing the potential for misuse.

## CHALLENGES OF SURVEILLANCE TECHNOLOGY AND ITS SOLUTIONS FROM AN ISLAMIC PERSPECTIVE

The rapid development of surveillance technology, such as CCTV cameras with facial recognition, mobile phone location tracking, and online activity monitoring, has posed serious challenges in safeguarding individual privacy and digital rights. While this technology has potential benefits in maintaining security and order, its uncontrolled use can threaten individual freedom and lead to other negative consequences.

### 1. Threats of Surveillance Technology

a. Privacy Violations:

Advanced surveillance technologies can collect and analyze individuals' personal data on a massive scale and without their knowledge. This can violate individuals' privacy rights and raise the risk of data misuse, such as identity theft, discrimination, and manipulation.(Andika & M. Soemarno, 2023)

Uncontrolled use of surveillance technology can threaten freedom of expression and opinion. Individuals may feel intimidated or afraid to express their views openly if they feel constantly monitored. This can hinder public participation in democratic processes and narrow the space for healthy discourse. Therefore, it is essential to ensure that the use of surveillance technology is

strictly regulated and transparent, taking into account ethical principles and human rights.

b. Discrimination:

Surveillance technologies that utilize certain algorithms, such as facial recognition, can lead to bias and discrimination against specific groups. For example, facial recognition algorithms that are not trained on diverse data can produce higher error rates for minority groups, leading to discrimination in law enforcement or public services.(Chen, 2023)

Furthermore, the massive use of surveillance technology also has the potential to violate individual privacy rights. Personal data collected through surveillance cameras, location tracking, or social media monitoring can be misused for unethical purposes, such as political manipulation, discrimination, or even identity theft. Therefore, it is crucial to ensure that there are clear and strict regulations regarding the use of surveillance technology, as well as independent oversight mechanisms to prevent misuse and protect individual rights.

c. Data Misuse:

Data collected through surveillance technology can be misused for unethical or illegal purposes. For example, personal data may be sold to third parties without the owner's consent, or used to spy on and intimidate specific individuals or groups.(Anggen Suari & Sarjana, 2023)

The unchecked use of surveillance technology can threaten freedom of expression and opinion. Individuals may feel intimidated to express dissenting views or criticize government policies, fearing potential consequences arising from surveillance. This can hinder the development of democracy and public participation in decision-making processes.

## 2. Islamic Solutions for Addressing the Challenges of Surveillance Technology

Islam offers a comprehensive solution to address the challenges of surveillance technology, emphasizing the principles of ethics, justice, and the common good.

a. Strict Regulation:

Islam advocates for strict regulation of the use of surveillance technology. This regulation should include clear limitations on the types of data that can be collected, the purpose of its use, and independent oversight mechanisms. (Kusuma, 2023) The regulation must also ensure transparency and accountability in the use of surveillance technology, as well as provide legal protection for individuals whose privacy rights are violated.

In addition to strict regulations, Islam also encourages dialogue and collaboration among various stakeholders in formulating surveillance technology policies. This includes involving religious scholars, technology experts, academics, human rights activists, and the general public.(Sugiharto & Syaifullah, 2023) The goal is to create a balance between security needs and the protection of human rights in the use of surveillance technology. Thus, regulations are not only effective but also reflect the ethical values and justice upheld in Islam.

b. Ethical Technology Development:

Islam encourages the development of surveillance technology that respects privacy and ethics. This technology should be designed to minimize unnecessary data collection and avoid bias and discrimination in the algorithms used. Furthermore, surveillance technology should be used proportionally and only for legitimate purposes that align with legal and ethical principles.(Andika, 2022)

Transparency and accountability are also fundamental principles in the Islamic perspective on surveillance technology. The public has the right to know how their data is collected, stored, and used.(Sudaryanti, 2011) Furthermore, independent and effective oversight mechanisms must be implemented to ensure that surveillance technology is not misused and remains in accordance with prevailing ethical and legal principles. Thus, Islam not only provides an ethical foundation but also practical guidance for the development and use of responsible and sustainable surveillance technology.

c. Public Awareness Enhancement:

It is crucial to raise public awareness regarding their digital rights, the risks associated with surveillance technology, and the importance of responsible technology use. Public education on these issues can empower individuals to be

more critical of surveillance technology usage and demand better protection from the government and corporations.

Collaboration among the government, private sector, academia, and civil society is essential in developing effective and equitable cyber regulations. This multi-stakeholder approach can ensure that the resulting policies consider diverse perspectives and interests, making them more comprehensive and sustainable. Furthermore, it is important to involve the public in the policy-making process to ensure that the regulations align with the needs and aspirations of the community.

## CASE STUDY: IMPLEMENTATION OF CYBER REGULATIONS AND SURVEILLANCE TECHNOLOGY IN MUSLIM-MAJORITY COUNTRIES

To further understand how Islamic principles are applied in cyber regulation and the use of surveillance technology, let's examine some case studies from countries with Muslim-majority populations. These case studies will provide insights into the successes and challenges of implementing Islamic values in the digital age.

1. **United Arab Emirates (UAE):**

   The UAE has become a pioneer in the development of comprehensive cyber regulations. The UAE Cyber Law of 2012 governs various aspects of cybersecurity, including personal data protection, prohibition of harmful content, and handling of cybercrime. The law also establishes a specialized supervisory body to ensure the effective implementation of regulations. However, the UAE has also faced criticism regarding its use of strict surveillance technology, particularly in terms of monitoring online activities and restricting freedom of expression.(Younies & Al-Tawil, 2020)

   On the other hand, the UAE's approach to cyber regulation has become an example for other countries in the Middle East and North Africa region. Several countries have adopted elements of the UAE Cyber Law in developing their own regulations. However, it is important to note that the social and political context of each country is different, so the implementation of cyber regulations must be adapted to the needs and values of each country. The main challenge in adopting

the UAE model is finding a balance between cybersecurity, personal data protection, and freedom of expression.(Al-Qudsi & Abu-Shanab, 2021)

2. **Malaysia:**

   Malaysia has the Personal Data Protection Act 2010, which governs the collection, use, and disclosure of personal data. This law aligns with Islamic principles regarding privacy protection and individuals' rights over their data. However, the implementation of this law still faces challenges, particularly in terms of law enforcement and public awareness of their digital rights.((JPDP), 2021)

   The rapid advancement of technology has also brought forth new challenges in the implementation of the Personal Data Protection Act 2010 in Malaysia. Issues such as the use of artificial intelligence, big data analytics, and online tracking require more specific regulatory adjustments. Therefore, continuous efforts are needed to review and update the law to ensure its relevance in the ever-evolving digital landscape. Collaboration between the government, private sector, and civil society is also crucial to ensure effective and comprehensive personal data protection implementation in Malaysia.((JPDP), 2021)

3. **Saudi Arabia:**

   Saudi Arabia has invested heavily in surveillance technology, including the use of facial recognition cameras and social media monitoring. This technology is used to maintain security and order but also raises concerns about privacy violations and restrictions on freedom of expression. The Saudi Arabian government claims that the use of surveillance technology is in accordance with Islamic law, but critics argue that it can be misused for political purposes and violate human rights.(Alzahrani & Alshammari, 2023)

   Saudi Arabia has made significant investments in surveillance technology, utilizing facial recognition cameras and social media monitoring. While this technology is deployed with the stated goal of maintaining security and order, it has also raised concerns regarding privacy violations and restrictions on freedom of expression. The Saudi government maintains that the use of surveillance technology aligns with Islamic law, but critics contend that it can be misused for political gain and infringe upon human rights.

4. **Indonesia:**

   Indonesia has enacted the Electronic Information and Transactions Law (UU ITE), which regulates various aspects of electronic transactions and online content. The law also includes articles on personal data protection and prohibitions against harmful content. However, the UU ITE has also drawn controversy as some of its articles are considered to restrict freedom of expression and have been used to criminalize criticism of the government.(Utin Indah Permata Sari, 2022)

   In addition to the Electronic Information and Transactions Law (UU ITE), Indonesia also has other regulations related to surveillance technology, such as the Government Regulation on the Implementation of Electronic Systems and Transactions (PP PSTE), which further regulates the protection of personal data and information security. However, the implementation of these regulations still faces challenges, such as a lack of public awareness of their digital rights and limited law enforcement capacity in handling cybercrime. Therefore, it is important for the government and other stakeholders to continue strengthening the regulatory framework and improving digital literacy among the public so that surveillance technology can be used ethically and responsibly.

From the case study above, it can be concluded that the application of Islamic principles in cyber regulation and the use of surveillance technology still faces various challenges. These challenges include:

1. **The Balance Between Security and Privacy:**

   Governments often face a dilemma between safeguarding national security and protecting individual privacy. Excessive use of surveillance technology can threaten privacy and individual freedoms, while overly lax regulations can endanger national security.

   Finding common ground between security and privacy is a crucial challenge in formulating effective cyber regulations. It is essential to design policies that not only protect national interests but also guarantee individuals' rights to privacy and freedom of expression. Transparency in the use of surveillance technology, independent oversight of surveillance activities, and effective

complaint mechanisms can be important steps in achieving this balance. Collaboration between the government, civil society, and the private sector is also necessary to ensure that resulting cyber regulations are not only effective but also fair and respectful of human rights.

2. **Law Enforcement:**

   Well-crafted cyber regulations will be ineffective without strict and consistent law enforcement. Challenges in law enforcement include lack of resources, corruption, and political intervention.

   The complexity of cyberspace also presents a unique challenge in law enforcement. Cybercrimes are often transnational, involving perpetrators and victims from different countries. This requires strong and effective international cooperation in tracking and prosecuting cybercriminals. Moreover, the rapid advancement of technology demands that law enforcement agencies continuously enhance their capacity and skills in understanding and addressing various increasingly sophisticated cybercrime methods.

3. **Public awareness:**

   The public needs to have a good understanding of their digital rights, the risks of surveillance technology, and the importance of using technology responsibly. A lack of public awareness can make them vulnerable to technology abuse and privacy violations.

To address these challenges, a comprehensive approach to improving digital literacy is necessary, encompassing education about digital rights, ethical technology use, and how to protect oneself from the risks of misuse. Collaboration between the government, educational institutions, and civil society organizations is crucial in building public awareness that is critical and responsible towards technology. Thus, the public can become active agents of change in promoting the ethical use of surveillance technology that respects human rights.

To address these challenges, a collaborative effort is needed from the government, non-governmental organizations, academics, and society as a whole. Several steps that can be taken include:

1. **Development of comprehensive and balanced regulations:**

Cyber regulations should be comprehensive, covering all aspects of cybersecurity, personal data protection, and the use of surveillance technology. The regulations should also be balanced, taking into account national security interests and individual rights.

Cyber regulations need to be adaptive and responsive to the rapid pace of technological developments. This means that regulations must be able to keep up with the dynamics of technology and evolving cyber threats, and can be revised periodically to ensure their effectiveness. In addition, transparency and public participation are also important in the development of cyber regulations. By involving various stakeholders, including technology experts, academics, human rights activists, and the general public, it is expected that the resulting regulations will be more comprehensive, balanced, and in line with the needs of society.

2. **Strengthening Law Enforcement:**

The government needs to strengthen law enforcement against violations of cyber regulations. This can be done by increasing resources, training, and coordination among law enforcement agencies.

International cooperation also needs to be enhanced in handling cross-border cybercrimes. The exchange of information, digital evidence, and expertise between countries can strengthen law enforcement efforts globally. The government also needs to encourage active public participation in reporting violations of cyber regulations, as well as raise public awareness of the importance of security and ethics in cyberspace.

3. **Raising public awareness:**

The government and relevant institutions need to educate the public about digital rights, the risks of surveillance technology, and digital ethics. This education can be carried out through various means, such as public campaigns, training programs, and educational curricula.

In addition to education, there also needs to be an effective reporting and handling mechanism for digital rights violations. This could include the establishment of an independent body tasked with overseeing the use of surveillance technology, as well as providing access to justice for victims of

digital rights violations. It's also important to encourage public participation in the formulation of policies related to surveillance technology, so that these policies can accommodate the interests and values held by the public.

By overcoming these challenges, it is hoped that Islamic principles can be implemented more effectively in cyber regulation and the use of surveillance technology, thus creating a digital environment that is safe, fair, and beneficial for all of society.

## BUILDING TRUST IN THE DIGITAL WORLD: ESSENTIAL SOLUTIONS FOR A SECURE, THRIVING, AND SHARIA-COMPLIANT ONLINE ENVIRONMENT

Trust is a crucial foundation in every human interaction, including in the digital world that increasingly dominates modern life. The absence of trust can hinder digital economic growth, erode social cohesion, and threaten the security of individuals and society. In the Islamic context, building trust in the digital world is not merely a practical necessity but also a moral obligation rooted in the noble values of the religion.

### 1. Principles of Faith in Islam: The Foundation for Digital Ethics

Islam offers a comprehensive ethical framework to guide human behavior in all aspects of life, including the digital world. Key principles relevant to building trust in the digital realm include:

a. Amanah (Trust):

The concept of amanah in Islam emphasizes the importance of upholding the trust bestowed upon us, both in worldly and spiritual matters. Allah SWT states in the Quran, "Indeed, Allah commands you to render trusts to whom they are due." (QS. An-Nisa: 58)(Amiruddin, 2021) In the digital context, amanah means safeguarding users' personal data, not misusing information entrusted to us, and fulfilling promises made in online transactions.

Applying the principle of amanah in the digital world also means being responsible for the content we share on social media. We must ensure that the information we share is accurate and beneficial, does not contain slander or hate

speech that could harm others. Additionally, amanah requires us to respect copyright and refrain from distributing illegal content. By upholding the value of amanah, we can create a digital space that is safe, positive, and beneficial for all users.

b. Sidq (Honesty):

Honesty is one of the main pillars in Islam. The Prophet Muhammad (peace be upon him) said, "You should always be honest, because honesty will lead to goodness, and goodness will lead to paradise." (Narrated by Bukhari and Muslim).(Madani, 2021) Honesty in the digital world means conveying information that is true and accurate, not spreading false news or hoaxes, and not committing fraud in online transactions.

Furthermore, honesty in interacting online also includes not committing plagiarism, respecting copyright, and not spreading harmful or slanderous content. In Islam, guarding one's tongue and writing from lies and slander is the obligation of every Muslim. Thus, honesty in the digital world is not just an ethical value, but also part of worship that is rewarded by Allah SWT.

c. Justice:

Islam upholds the principle of justice in all matters. Allah SWT says, "And when you judge between people, judge with justice." (QS. An-Nisa: 58).(Fatihin, 2017) Justice in the digital world means treating all users fairly and equally, without discrimination based on religion, race, ethnicity, or gender, and providing equal opportunities for everyone to access and utilize digital technology.

Justice in the digital context also means ensuring that every individual has equal access to information and digital services, as well as protection from any form of technology misuse that could harm them. In this regard, the role of fair and transparent cyber regulations is crucial in creating an inclusive and equitable digital environment for the entire community. Furthermore, the value of justice also encourages the use of digital technology for purposes that benefit humanity, such as education, health, and economic empowerment.

d. Ihsan (Goodness):

The concept of ihsan in Islam means doing good to fellow humans and other creatures. The Prophet Muhammad (peace be upon him) said, "Worship Allah as if you see Him, and if you cannot see Him, then indeed He sees you." (Narrated by Bukhari and Muslim).(Ahmad Mujahid & Haeriyyah, 2020) Ihsan in the digital world means using technology for good and beneficial purposes, not using it to harm or hurt others, and contributing to creating a positive and constructive online environment.

The application of ihsan in the digital world also means respecting the copyrights and intellectual property of others, not spreading fake news or hoaxes, and not engaging in cyberbullying or hate speech. In a broader context, ihsan encourages Muslims to use technology as a means to improve the quality of life for society, such as developing educational, health, or environmental applications. Thus, ihsan becomes an important ethical principle in realizing a digital world based on the values of goodness and humanity.

**2. The Application of Islamic Principles in Building Trust in the Digital World .**

These Islamic principles can serve as a strong ethical foundation for designing and implementing solutions to build trust in the digital world. Some concrete steps that can be taken include:

a. Development of Regulations Based on Islamic Values:

The government and other stakeholders need to develop comprehensive cyber regulations that align with Islamic values. These regulations should encompass personal data protection, prohibition of harmful content, and the promotion of technology use for the common good. Additionally, the regulations need to address specific aspects relevant to the Islamic context, such as the prohibition of riba (usury) in online transactions and the protection of religious values in digital content.

It is also crucial to involve Islamic scholars and intellectuals in the process of formulating these cyber regulations. They can provide valuable insights and advice based on Islamic principles, ensuring that the regulations are consistent with religious values and ethics. Furthermore, public education on Islamic ethics

and laws regarding technology use needs to be enhanced. This will raise awareness among the public about their responsibility to use technology responsibly and in accordance with religious values.

b. Enhancing Digital Literacy and Islamic Ethics:

Education about digital literacy and Islamic ethics needs to be strengthened across all levels of society. This can be achieved through various means, such as incorporating digital ethics into educational curricula, conducting training workshops and seminars, and disseminating information through social media and other online platforms. Improving digital literacy and Islamic ethics will empower individuals to use digital technology more wisely and responsibly, while also fostering greater sensitivity to ethical and moral issues related to the digital world.

Collaboration between the government, educational institutions, religious leaders, and online communities is also crucial in creating a healthy and ethical digital ecosystem. Through this cooperation, educational platforms and content that align with Islamic values can be developed, and constructive dialogue and discussion about digital ethics can be encouraged. This will enable people to better understand how to apply Islamic principles in their digital lives, leading to a safer, more beneficial, and ethically sound cyberspace that reflects the noble values of the religion.

c. Sharia-Compliant Technology Development:

The development of digital technology must consider Islamic principles. This can be achieved by involving religious scholars and experts in the technology development process, ensuring that the resulting technology does not conflict with Islamic values. For example, developing a sharia-compliant e-commerce platform can avoid usury (riba) and ensure that offered products and services are halal and align with Islamic principles.

The application of digital technology in Islamic finance also needs to adhere to Islamic principles. For instance, developing sharia-compliant banking applications can help Muslims manage their finances in accordance with Islamic principles, such as avoiding riba and ensuring halal investments. In this way,

digital technology can serve as a means to expand public access to sharia-compliant financial services that align with religious values.

d. Collaboration between Government, Private Sector, and Civil Society:

Building trust in the digital world requires collaboration from all stakeholders. The government needs to create a supportive regulatory framework, the private sector needs to develop ethical and responsible technology, and civil society needs to play an active role in monitoring and providing input on policies and practices related to the digital world.

By applying Islamic principles in building trust in the digital world, we can create a safe, thriving online environment that aligns with the noble values of the religion. This will bring significant benefits to individuals, society, and the Muslim community as a whole.

## 5. CONCLUSION

This research has revealed the urgency of building trust in the increasingly complex digital world, which is vulnerable to misuse. The Islamic perspective, with its noble values such as trust (amanah), honesty, justice, and benevolence (ihsan), offers a solid ethical foundation to guide the actions of individuals and society in utilizing digital technology.

These Islamic principles can be implemented in various aspects of digital life, ranging from the development of comprehensive and ethical cyber regulations, the improvement of digital literacy and Islamic ethics in society, to the development of technology that aligns with Islamic law (sharia). Collaboration between the government, the private sector, and civil society is also crucial in creating a digital environment that is safe, fair, and beneficial for all.

Recommendations for Cyber Regulation Development:

1. Comprehensive and Values-Based Regulation:

Cyber regulations should encompass all aspects of digital life, including personal data protection, online transaction security, prohibition of harmful content, and responsible use of surveillance technology. Regulations should also be based on Islamic values, such as justice, public interest, and respect for human dignity.

2. Firm and Fair Law Enforcement:

   Good regulations will not be effective without firm and fair law enforcement. The government needs to strengthen the capacity of law enforcement agencies in dealing with cybercrime and other regulatory violations. Additionally, law enforcement must be carried out fairly and without discrimination.

3. Public Participation:

   The public needs to be involved in the formulation and implementation of cyber regulations. Public participation can be done through public consultations, discussion forums, and effective complaint mechanisms. In this way, the resulting regulations will be more in line with the needs and aspirations of the community.

Suggestions for Addressing the Challenges of Surveillance Technology

1. Ethical and Responsible Technological Development:

   Developers of surveillance technology must prioritize ethical principles and social responsibility. Surveillance technology should be designed to minimize negative impacts on privacy and human rights. Furthermore, the use of surveillance technology must be transparent and accountable.

2. Raising Public Awareness of Digital Rights:

   The public needs to be adequately informed about their digital rights, including the right to privacy and personal data protection. This will enable individuals to be more critical of surveillance technology use and demand better protection from governments and corporations.

3. Independent Monitoring and Evaluation:

   The use of surveillance technology should be monitored and evaluated independently by credible institutions. This monitoring and evaluation is crucial to ensure that surveillance technology is used for legitimate purposes and not misused for specific interests.

By implementing the aforementioned recommendations and suggestions, it is hoped that a safer, fairer, and more sustainable digital environment can be created, one that aligns with Islamic values and benefits all of humanity.

## DAFTAR REFERENSI

(JPDP), J. P. D. P. M. (2021). *Personal Data Protection Act 2010: A Review of Its Implementation and Challenges*. https://www.pdp.gov.my/jpdpv2/laws-of-malaysia-pdpa/personal-data-protection-act-2010/?lang=en

Ahmad Mujahid, & Haeriyyah. (2020). Interpretasi Ayat-Ayat Ihsān Dalam Pengembangan Hukum Islam. *Jurnal Mazahibuna*, *2*(2), 270–283.

Al-Qudsi, S., & Abu-Shanab, A. (2021). Cybercrime Legislation in the United Arab Emirates: A Critical Analysis. *Journal of Internet Law*, *24*(2), 1–26.

Almujaddedi, M. ., & Hayati, R. (2022). Perspective of Islamic Law on Hate Comments in Social Media. *JCH (Jurnal Cendekia Hukum)*, *7*(2), 243. https://doi.org/10.33760/jch.v7i2.466

Alzahrani, S., & Alshammari, A. (2023). The Evolution of Surveillance Technologies in Saudi Arabia: A Critical Analysis of Privacy, Security, and Human Rights Implications. *Journal of Cyber Policy*, *5*(2), 23-40.

Amiruddin, A. (2021). AMANAH DALAM PERSPEKTIF AL-QURAN (Studi Komparatif Tafsir Al-Misbah dan Al-Azhar). *Jurnal MUDARRISUNA: Media Kajian Pendidikan Agama Islam*, *11*(4), 833. https://doi.org/10.22373/jm.v11i4.4665

Ananda, R. R. (2023). *Hak Asasi Manusia di Ranah Digital: Analisis Hukum Siber dan Kebebasan Online*. Westscience Press.

Andika, A. (2022). Agama Dan Perkembangan Teknologi Di Era Modern. *Abrahamic Religions: Jurnal Studi Agama-Agama*, *2*(2), 129. https://doi.org/10.22373/arj.v2i2.12556

Andika, & M. Soemarno. (2023). Masalah Privasi dan Keamanan Data Pribadi pada Penerapan Kecerdasan Buatan. *INNOVATIVE: Journal Of Social Science Research*, *3*, 4917–4929.

Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142. https://doi.org/10.38043/jah.v6i1.4484

Angriani, P. (2021). Perlindungan Hukum terhadap Data Pribadi dalam Transaksi E-Commerce: Perspektif Hukum Islam dan Hukum Positif. *DIKTUM: Jurnal Syariah Dan Hukum*, *19*(2), 149–165. http://ejournal.bsi.ac.id/ejurnal/index.php/cakrawala

Chen, Z. (2023). Ethics and discrimination in artificial intelligence-enabled recruitment practices. *Humanities and Social Sciences Communications*, *10*(1). https://doi.org/10.1057/s41599-023-02079-x

DataProt. (2023). *Global Survey Reveals Widespread Concern About Data Privacy*. DataProt. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2023.pdf

Fatihin, R. (2017). Keadilan Sosial dalam Perspektif Al-Qur'an Dan Pancasila. *Panangkaran: Jurnal Penelitian Agama Dan Masyarakat*, *1*(2), 293. https://doi.org/10.14421/panangkaran.2017.0102-06

Khansa, F. N. (2021). Penguatan Hukum dan Urgensi Otoritas Pengawas Independen dalam Pelindungan Data Pribadi di Indonesia. *Jurnal Hukum Lex Generalis*, *2*(8), 649–662. https://doi.org/10.56370/jhlg.v2i8.114

Kusuma, K. A. (2023). Buku Ajar Pengantar Bisnis Digital dalam Perspektif Islam. In *Buku Ajar Pengantar Bisnis Digital dalam Perspektif Islam*. https://doi.org/10.21070/2023/978-623-464-070-0

M. Syafii Maarif. (2022). *Hukum Siber dan Perlindungan Data Pribadi dalam Perspektif Islam*. Pustaka Cendekia Utama.

Madani, H. (2021). Pembinaan Nilai-nilai Kejujuran Menurut Rasulullah Saw. *Jurnal Riset Agama*, *1*(1), 145–156. https://doi.org/10.15575/jra.v1i1.14346

Marzuki, P. M. (2014). Penelitian Hukum. In *Kencana Prenada Media Group*. Kencana Prenada Media Group.

Putra, I. G. N. (2023). *Membangun Kepercayaan di Era Masyarakat Digital*. Gadjah Mada University Press.

Rosidah, I., Gunardi, Priatna Kesumah, & Royke Bahagia Rizka. (2023). Transparasi Dan Akuntabilitas Dalam Pencegahan Fraud Diinstansi Pemerintah (Studi Kasus Kantor Kec. Ciwidey). *Jurnal Ekonomi Manajemen Bisnis Dan Akuntansi : EMBA*, *2*(1), 137–156. https://doi.org/10.59820/emba.v2i1.110

Sudaryanti, D. (2011). Akuntabilitas dalam Perspektif Islam: Solusi Masalah Korupsi

di Indonesia. *Tera Ilmu Akuntansi*, *10*(1), 58–76.

Sugiharto, B., & Syaifullah, M. (2023). Pengawasan dalam Perspektif Islam dan Manajemen. *ILTIZAM Journal of Shariah Economics Research*, *7*(1), 124–132. https://doi.org/10.30631/iltizam.v7i1.1878

Suprapto, A., & Yulianto. (2023). Pandangan Islam Terhadap Pengembangan. *Journal of Islamic Integration Science and Technology*, *I No I*(I), 1–26. http://ejournal.uin-malang.ac.id/index.php/essyajar/index%0APandangan

Syafuddin, K., Jamalullail, & Rafi'i. (2023). Peningkatan Literasi Keamanan Digital Dan Perlindungan Data Pribadi Bagi Siswa Di Smpn 154 Jakarta. *Eastasouth Journal of Impactive Community Services*, *1*(03), 122–133. https://doi.org/10.58812/ejimcs.v1i03.119

Utin Indah Permata Sari. (2022). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Jurnal Studia Legalia*, *2*(01), 58–77. https://doi.org/10.61084/jsl.v2i01.7

Wahyuningati, & Utami, S. T. (2023). Perlindungan Data Pribadi dalam Perspektif Islam: Tinjauan Normatif dan Praktis. *Jurnal Hukum Islam UIN Maulana Malik Ibrahim Malang*, *10*(2), 243–260.

Waluya, A. H., & Mulauddin, A. (2021). AKUNTANSI: AKUNTABILITAS DAN TRANSPARANSI DALAM QS. AL BAQARAH (2): 282-284. *MUAMALATUNA*, *12*(2), 15–35. https://doi.org/10.37035/mua.v12i2.3708

We Are Social Digital. (2023). *DIGITAL 2023*. https://wearesocial.com/id/blog/2023/01/digital-2023/

Younies, H., & Al-Tawil, T. N. (2020). Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). *Journal of Financial Crime*, *27*(4), 1089–1105. https://doi.org/10.1108/JFC-04-2020-0055