THE PHENOMENON OF ONLINE CONSUMER DATA SECURITY IN ISLAMIC VALUE-BASED DIGITAL ETHIC

by Afriyan Aryasaputra

Submission date: 30-Oct-2021 06:52AM (UTC+0700)
Submission ID: 1688002553
File name: CONSUMER_DATA_SECURITY_IN_ISLAMIC_VALUE-BASED_DIGITAL_ETHIC.docx (131.76K)
Word count: 4364
Character count: 26111

Received: 00 Month 20xx; Revised: 00 Month 20xx; Accepted: 00 Month 20xx

THE PHENOMENON OF ONLINE CONSUMER DATA SECURITY IN ISLAMIC VALUE-BASED DIGITAL ETHIC

Afriyan Arya Saputra[1*]
Muhammad Iqbal Fasa[2]
Diana Ambarwati[3]
[1,3]IAIN Metro Lampung
[2]UIN Raden Intan Lampung
[*]*Corresponding Email*: afriyanaryasaputra@gmail.com

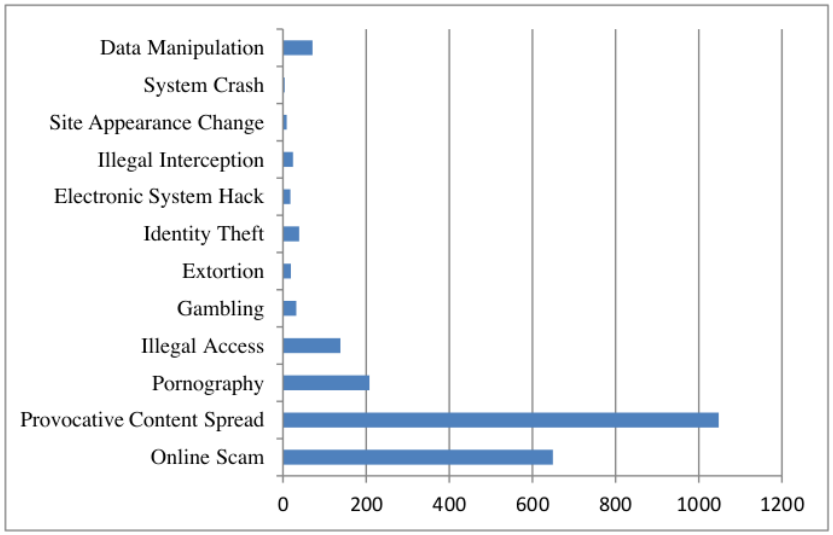
ABSTRACT - Cyber security is a vital issue because it threatens the security of consumer data. Technology and the development of cyber security frameworks are sought to be able to mitigate and minimize the occurrence of data theft and cyber-attacks. This study aims to examine the role of digital ethics based on Islamic values in cyber security. The findings in this study show that ethics influence behavior. Digital ethics plays a role as morality control in the digital space. Where digital ethics based on Islamic values place online consumers as independent internet users, having the authority to maintain the privacy and security of their data. Ethics in cyberspace plays a role in digital security. This study proposes that the inculcation of these values can be started through Islamic educational institutions.
Keywords: Cyber Security, Digital Space, Digital Ethics, Islamic Value

ABSTRAK – Fenomena Keamanan Data Konsumen Online Dalam Etika Digital Berbasis Nilai Islam. *Keamanan siber merupakan isu vital karena mengancam keamanan data konsumen. Teknologi dan pembangunan framework keamanan siber diupayakan mampu memitigasi dan meminimalisir terjadinya pencurian data dan serangan siber. Penelitian ini bertujuan untuk menelaah peranan etika digital berbasis nilai Islam dalam keamanan siber. Temuan dalam penelitian ini menunjukkan etika memengaruhi perilaku. Etika digital berperan sebagai kontrol moralitas di ruang digital. Di mana etika digital berbasis nilai Islam menempatkan konsumen online sebagai pengguna internet yang merdeka, memiliki otoritas dalam menjaga privasi dan keamanan datanya. Etika di ruang siber ikut berperan dalam keamanan digital. Penelitian ini mengusulkan, penanaman nilai tersebut dapat dimulai melalui lembaga pendidikan Islam. disarankan penelitian lanjutan mengenai etika digital berbasis nilai Islam dengan fenomena digital yang beragam dan pendekatan penelitian partisipan.*
Kata Kunci: *Keamanan Siber, Ruang Digital, Etika Digital, Nilai Islam*

INTRODUCTION

The threat of online consumer data security is increasingly worrying. There are at least two cases that stick out, first, in mid-2020, Startexmislead accounts offered 12,957,573 data on the dark web Raid Forum. Second, in mid-2021, the owner of the Kotz account sold 279 million Indonesian population data in the same forum. Based on Cyber Patrol statistics, from January to December 2020 there were 2,259 reports from the public regarding cybercrimes (see Graph 1). Based on research by (Mohamed & Ali, 2020) cybersecurity can be improved by tightening surveillance and adopting advanced technologies.

Graph 1. Cybercrime Trends in Indonesia



Source: (Siber, 2020)

So far, studies on online consumer data security have focused more on two aspects. First, a study that discusses the role of technology in cybersecurity systems (Craigen et al., 2014; Herdiana et al., 2021; Mujeeb-ur-Rehman et al., 2021; Naseer et al., 2021). Second, the focus of the study is on the mitigation and development of cyber security frameworks (Amatullah et al., 2020; Mylrea et al., 2018; Nafi'ah, 2020). The tendency of studies on these two aspects ignores the position of digital ethics based on Islamic values. Where interactions in the digital space are closely related to behavioral values.

The purpose of this paper is to complete the understanding of cyber security in a review of digital ethics based on Islamic values. This study specifically describes a review of Islamic values-based digital ethics on the data security of consumers who conduct online transactions. In line with this, three questions can be formulated: (a) What is the role of cybersecurity in protecting consumer data? (b) What factors ensure the privacy of online consumer data? (c) How do ethical principles in Islam view the security of online consumer data? The answers to these three questions will explain the important position of online consumer data security in a review of Islamic values-based digital ethics.

This paper is generally based on three arguments. First, cybersecurity protects consumer data. Second, online consumer data privacy is largely determined by digital ethical factors. Support for ethical behavior is a determinant in preventing crime in the digital world. Third, online consumer data security that prioritizes digital ethics will not be realized without prioritizing Islamic values from consumers who make online transactions.

LITERATURE REVIEW

Cyber Security

Cyber security is security in information technology that focuses on protecting hardware, software, and data contained in an internet-connected system from illegal access and cyber-attacks (Dixit & Silakari, 2021; Mago, 2014). In addition, cybersecurity systems must be supported by cybersecurity knowledge in conducting attribution assessments which are the basis for security for internet users from cyber threats (Egloff & Cavelty, 2021). According to (Corallo et al., 2021), cyber security is not just on information technology (IT) systems because it affects the entire ecosystem in operational technology (OT) which interacts directly with the physical world. Furthermore,(Rachman & Susan, 2021) stated that cyber security is not limited to threats related to technology issues but departs from the threat of radical awareness from the digital community.

The issue regarding cybersecurity is growing across the country. The use of the internet in a country opens up opportunities for cyber attacks, therefore resources or a system are needed to protect cyberspace, the system is known as cybersecurity (Craigen et al., 2014). There are five core elements of the Buildings Cybersecurity Framework (BCF) which refer to the National



Institute of Standards and Technology (NIST) in building critical infrastructure, namely: identity, protect, detect, respond, and recover. Mylrea et al. (2018) explained: (1) Identify has a function in identifying various cybersecurity threats and weaknesses; (2) Protect functions to recommend handling in managing cyber risk; (3) Detection focuses on techniques, policies, and procedures in detecting cyber-attacks; (4) Respond focuses on handling in responding to cybersecurity incidents; while (5) Recover focuses more on restoring normal operating services.

Study (Desy Komalawati et al., 2021) said that the level of cyber security in Indonesia is still low, which makes it possible for consumer data theft to occur. Based on the Databoks Report 2020, there were 105.2 million e-commerce user data stolen, where the data were in the form of names, e-mails, and passwords.

Threat cyber attacks like theft data show the urgency of the reliability of the cybersecurity system. Because, all internet users have the right to privacy and are free without social pressure (Burgoon, 1982) and being spied on by any party (Widiantari, 2021). For that, referring to Peraturan Badan Siber Dan Sandi Negara Nomor 8, 2020 the importance of electronic system operators (public and private) to ensure the security of information management. Thus, electronic system operators can develop cyber security that prioritizes cyber security principles to protect privacy and consumer rights, such as the use of one-time passwords, personal identification numbers (PINs), end-to-end data exchange, and increased system surveillance (Amatullah et al., 2020), and the application of advanced encryption techniques (Nafi'ah, 2020).

Islamic Value-Based Digital Ethics

Digital ethics are normative principles in carrying out an action and interacting in the digital space (Luke, 2018). According to (Kusumastuti et al., 2021) ethics in the digital space relates to actions and all interactions that are based on behavior that is full of awareness, responsibility, honesty, and benevolence, where this behavior leads to improving the quality of humanity. The form of action and interaction in the digital space can be seen in three patterns of relationships, namely individuals, between individuals, and communities—which all three live a life model by utilizing digital space as a means of mediation (Pilliang, 2012).



Ethics in the digital space is a necessity that cannot be ruled out. Ethical behavior in the digital space can prevent internet users from distrust, hatred, conflict, and the misuse of digital tools that can cause huge losses (Véliz, 2019). According to (Floridi, 2016), ethics are able to control humans to act more morally and ethics are also able to create value in interactions so that they are more valuable. In addition to ethics, a person's belief in his religion can build ethical behavior in the digital space. (Chaudhary, 2020) explains the value of Islamic teachings placing the individual as a moral subject who actualizes his personal behavior with full awareness and prioritizes moral aspects and responsibility. This ethical behavior is based on Islamic principles. There are five values that underlie ethical behavior in Islam, namely: (1) Unity of Command, the concept of monotheism about oneness; (2) Equilibrium and Balance, the concept of justice and balance between components and various aspects of life; (3) Freedom and Free will, the concept of human nature as the caliph of Allah SWT; (4) Benevolence or Ihsan, beneficial actions for others that are carried out without expecting anything in return; and (5) Responsibility (Mas'uliyyah), the concept of responsibility for all human actions to Allah SWT (Ahmad et al., 2021). These principles are the building of values based on the Qur'an and hadith. Furthermore, the actualization of Islamic values will result in ethical behavior in the digital space.

The value of monotheism, in this case, relates to activities worth worship. This means that every behavior or deed is intended as an effort to realize monotheism to Allah SWT. As the word of Allah in Surah Luqman: 30. The value of 'Adl means fair, honest, straight, and equates to something both in terms of size and value. The advice to be fair is as Allah Ta'ala in Surah An-Nahl: 90.

The value of being a caliph means that although he has free will in expressing his life activities, there are limits in human behavior. As caliphs, humans are required to prosper and spread prosperity throughout the world/earth by cooperating and helping each other (Surah An-Nahl: 90). This task places humans as components of a very large unity of creation. As in the word of Allah in Surah al-An’am: 165.

The value of virtue which is an ethical principle means to spread usefulness. The implementation of the value of Ihsan can be seen from the behavior of liking to do good. The word of Allah concerning the value of virtue in Surah al-Hajj: 77.



The value of responsibility, where all actions are taken will be held accountable both in this world (during life) and also in the hereafter. As the Word of Allah in Surah al-Hashr: 18.

METHODOLOGY

This study uses a qualitative approach, which is based on non-numeric data or data in the form of writing and images, and filtering of the data is carried out to make interpretations from the literature review (Creswell, 2014). The study in this study was conducted by examining the literature such as books, journals, reports, and other reliable sources. The data analysis technique used in this research is descriptive analysis.

RESULT AND DISCUSSION

Results

A. The Role of Cybersecurity in Protecting Consumer Data

Cyber security is needed along with the increasing activity of cyber threats. The high data theft of e-commerce users in Indonesia in 2020 in several marketplaces can be seen in the following table:

Table 1. Number of E-Commerce Data Theft

Nama	Banyak Data yang Dicuri
Tokopedia	91 Million
Bukalapak	13 Million
Bhinneka	1,2 Million

Source: (Databoks, 2020)

The existence of cyber threat activities comes from various actors, such as foreign intelligence actors, disappointed actors, investigations, extremist organizations, hacker activities (hacktivists), and activities from organized crime groups. The risks arising from cybercrime activities attack information data security systems that are connected to the internet network and can even result in a threat to a country's military activities (Rahmawati, 2017). Of course, these risks will affect the fabric of society, both real and virtual. Thus, cyber data theft is a serious problem facing today's digital society.

The data in Table 1. shows that cybersecurity needs to be tightened in order to protect the privacy of online consumer data. This form of security

enhancement is sole to protect privacy. To maximize the function of cybersecurity in protecting data privacy and digital assets, (Lee, 2021) explained the need to pay attention to the cyber ecosystem (stakeholders), evaluation of cyberinfrastructure (users, workforce, and technology), assessment of cyber risks (identification of devices, vulnerabilities, threats, and cyber attacks), and cybersecurity activities. According to (Naseer et al., 2021), cybersecurity innovation is needed towards the creation of integrated applications between threat intelligence data, automation of threat identification, forensic analysis, application of algorithms, and analysis of internet users. The urgency of developing cyber security for reliable data privacy security is very much needed.

Technological advances can be used to build cyber security. The adoption of advanced technology and algorithm upgrades on the system will have an impact on the accuracy of the security system (Herdiana et al., 2021), such as the adoption of internet of thing (IoT) based technology, blockchain, artificial intelligence (AI), avatar-based management technique, and other technologies. As expressed by (Mujeeb-ur-Rehman et al., 2021) adoption of advanced technology as cybersecurity is ideal for protecting the data privacy of internet users (clients, merchants, to online transaction systems) by implementing strict privacy security cycle stages. Internet user data privacy security is a very vital issue. So, the main focus of cybersecurity is protecting this privacy from illegal data access and the potential for abuse of it.

Supporting Factors of Online Consumer Data Privacy

The opportunities for cyber threats are directly proportional to the use of the internet. The potential for damage caused by cyber-attacks is getting higher. This is triggered by the misuse of technological advances by actors who launch cyber attacks. However, as in the previous discussion, technological advances can also be used to tackle crime in cyberspace.

The development of technology, infrastructure, and approach models for cybersecurity improvement continues. This effort is a response to a wider cyber threat. Cybersecurity protocols are seen as unable to fully ensure the security of internet users' privacy. On the other hand, technology integration with network changes such as 5G, IoT (Dawson et al., 2021), and AI (Djenna et al., 2021)) is considered capable of building a comprehensive, strategic and reliable cyberinfrastructure in dealing with cyber threats on a large exploitative scale.



In addition to technology, internet users also have a role to protect the privacy of their data. (Choo, 2011) Seeing the rapidly growing cyber threat landscape, advised stakeholders such as users, businesses, governments, and research institutions that rely on the internet to continue to innovate to tackle cyber threats such as data theft. Therefore, the element of internet users cannot be ruled out. Digital ethics for internet users influences their decisions in realizing threats in the digital space. (Floridi, 2018) explaining ethical behavior in the digital space can ensure users are aware of potential dangers, prioritize the precautionary principle, and mitigate risks because ethically compliant users can refuse data requests from malicious access. Ethical behavior is one of the key factors in pursuing a cybersecurity landscape where internet users are aware of each other's privacy. The provision of privacy and access to data for review is entirely in the privacy of each.

Islamic Value-Based Digital Ethics Viewing Online Consumer Data Security

The condition of internet users is increasingly worrying. (Hardiman, 2018) sees that internet users (digital society) act very brutally in the digital space. Such a situation, according to (Choiriyati & Windarsih, 2019) shows the need for ethical construction that is more knowledge in nature, which is extracted from religious values. In this regard, digital ethics based on Islamic values should be transformed conceptually to make it more applicable. (Chaudhary, 2020) explains the value of Islam can actualize the behavior of its adherents responsibly. Where Islamic ethics build a civilized and moral life.

Behavior and interactions are very important in Islam. Furthermore, internet users' awareness of data privacy and security in the digital space must be considered, because, in Islam, privacy is self-respect (Norwawi et al., 2014). Privacy is a basic right that must be respected. In Islam, with regard to privacy, it is closely related to granting permission. As the Word of Allah SWT in Surah an-Nur: 27-29.

The above paragraph emphasizes that permission is very important in privacy. In addition to the recommendation to ask for permission, there is also a prohibition against suspecting, spying and disseminating information belonging to others (slander). As the Word of Allah in Surah Al-Hujurat: 12.

The two verses above show that Islam is very concerned about privacy and security issues where the principle of confidentiality must be maintained. Ethical behavior is needed to safeguard data privacy issues in the digital space. (Faisal et al., 2013) said that service providers and application



developers need to pay attention to privacy issues, while for users, it is recommended to take a role in managing privacy by prioritizing Islamic values. This concern also applies to the security of online consumer data. (Imtiaz et al., 2020) that e-commerce that does not pay attention to the security of consumer data will lose consumer confidence. Furthermore, attention to the security of online consumer data privacy is very important in Islam.

Discussion

First: Cybersecurity protects consumer data.

Cybersecurity plays a role in protecting consumer data. However, this role is not effective. This is because various cyber threats to data protection and security adopt advanced technology. As a result, the issue of consumer data security has become a major issue in the digital world.

Adoption of technology in building cybersecurity will have an impact on cybersecurity that is increasingly reliable (Dawson et al., 2021; Djenna et al., 2021; Herdiana et al., 2021). Of course, this can be input for developers and internet service providers. Optimizing the protection of privacy and security of consumer data is needed to build a dignified cybersecurity landscape.

Second: Online consumer data privacy is determined by digital ethical factors based on Islamic values. Support for ethical behavior is a determinant in preventing crime in the digital space.

There are factors that influence the cybersecurity landscape, such as the infrastructure and technology used by service providers and application developers, as well as the ethical behavior of internet users. Ethics occupies a strategic position in maintaining behavior in the digital space. The urgency of Islamic values-based digital ethics is seen in the Islamic principle which requires its adherents to take advantage of the digital space so as not to harm themselves or others.

The guarantee of a sense of security interacting in the digital space can be started through each individual. Because in Islam, privacy is a value that must be equally respected (Norwawi et al., 2014). This confirms that with digital ethics based on Islamic values, the division of concentration is divided into individuals according to their portion. First, service providers and developers



improve cybersecurity infrastructure and technology. Second, consumers who make transactions (as internet users) prioritize their ethical behavior in the digital space.

Third: The security of online consumer data that prioritizes digital ethics based on Islamic values will not be realized without prioritizing the prudence of consumers who make online transactions.

Digital ethics plays the role of morality control in the digital space. Digital ethics based on Islamic values places online consumers as internet users who have the authority to maintain the security and privacy of their data. When online consumers are aware of cyber threats, they can prioritize the precautionary principle (Floridi, 2018), to make data transparency decisions. Furthermore, the precautionary principle is a key support in maintaining the security and privacy of consumer data. In this principle, consumers can be aware of their private areas. As well as the authority in giving decisions on the review of his personal data. Where these efforts are a support for the formation of a cybersecurity landscape.

CONCLUSIONS

It turns out that digital ethics based on Islamic values can be a means of moral development for internet users, especially consumers who make online transactions. This study shows that cybersecurity can be built through the cultivation of Islamic values-based ethics. The cultivation of these values can be started through educational institutions with an Islamic background. Through the inculcation of these values, consumers have independent authority in making decisions in an effort to protect their data. The decision, which is supported by ethical behavior in cyberspace, shows that the issue of cybersecurity is a problem that must be minimized together.

The use of digital ethics based on Islamic values in this research allows for a fundamental problem in cyber security. Infrastructure and technology in this study are seen as external instruments. Meanwhile, digital ethics based on Islamic values occupy an internal position, which can be fully controlled by individuals as moral consumers and internet users.

This research is limited to the use of philosophical ideas without testing them in reality through social experiments. This research only focuses on one problem so that there is limited understanding. A quantitative approach involving a wide range of participants allows for different results. From that,



it is recommended that further research on digital ethics based on Islamic values contains comparisons with other digital phenomena.

REFERENCES

Ahmad, K., Uluyol, B., & Altwijry, O. (2021). Contrast in Ethics , Morality , Justice , and Behavior : Some Reflections on Business. *Multidisciplinary Approaches to Ethics in the Digital Era*, *March*, 292–305. https://doi.org/10.4018/978-1-7998-4117-3.ch016

Amatullah, N., Rosadi, S. D., & Handayani, T. (2020). Perlindungan Konsumen dalam Transaksi Direct Carrier Billing Melalui Keamanan Siber. *Syiah Kuala Law Journal*, *4*(3), 323–337. https://doi.org/10.24815/sklj.v4i3.18967

Burgoon, J. K. (1982). Privacy and Communication. *Annals of the International Communication Association*, *6*(1), 206–249. https://doi.org/10.1080/23808985.1982.11678499

Chaudhary, M. Y. (2020). Initial Considerations for Islamic Digital Ethics. *Philosophy and Technology*, *33*(4), 639–657. https://doi.org/10.1007/s13347-020-00418-3

Choiriyati, W., & Windarsih, A. (2019). Etika Media Dalam Kultur New Technology (Mengkaji Etika Internet Versus Undang-Undang Informasi Dan Transaksi Elektronik) Media Ethics in New Technology Culture (Reviewing the Internet Ethics Versus the Information and Electronic Transaction Act). *Masyarakat & Budaya*, *21*(2), 247–262.

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers and Security*, *30*(8), 719–731. https://doi.org/10.1016/j.cose.2011.08.004

Corallo, A., Lazoi, M., Lezzi, M., & Pontrandolfo, P. (2021). Cybersecurity Challenges for Manufacturing Systems 4.0: Assessment of the Business Impact Level. *IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT*. https://doi.org/10.1109/TEM.2021.3084687

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/timreview835

Creswell, J. W. (2014). *Research design : qualitative, quantitative, and mixed methods approaches* (4th ed). SAGE Publications, Inc.

Databoks. (2020). *Bocornya Puluhan Juta Data Pengguna E-Commerce Indonesia*. https://databoks.katadata.co.id/datapublish/2020/05/12/bocornya-puluhan-juta-data-pengguna-e-commerce-indonesia

Dawson, M., Bacius, R., Gouveia, L. B., & Vassilakos, A. (2021).



Understanding the Challenge of Cybersecurity in Critical Infrastructure Sectors. *Land Forces Academy Review*, *26*(1), 69–75. https://doi.org/10.2478/raft-2021-0011

Desy Komalawati, M.R, M. D., & Kartika, R. D. (2021). KEJUTAN PULUHAN MILIAR TOKOPEDIA DITENGAH KASUS KEBOCORAN DATA. *Jurnal Syntax Admiration*, *2*(1), 49–56. https://doi.org/https://doi.org/10.46799/jsa.v2i1.167

Dixit, P., & Silakari, S. (2021). Deep Learning Algorithms for Cybersecurity Applications: A Technological and Status Review. *Computer Science Review*, *39*. https://doi.org/https://doi.org/10.1016/j.cosrev.2020.100317

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences (Switzerland)*, *11*(10). https://doi.org/10.3390/app11104580

Egloff, F. J., & Cavelty, M. D. (2021). Attribution and Knowledge Creation Assemblages in Cybersecurity Politics. *Journal of Cybersecurity*, *00*, 1–12. https://doi.org/10.1093/cybsec/tyab002

Faisal, A. A., Nisa', B. S., & Ibrahim, J. (2013). Mitigating privacy issues on Facebook by implementing information security awareness with Islamic perspectives. *2013 5th International Conference on Information and Communication Technology for the Muslim World, ICT4M 2013*. https://doi.org/10.1109/ICT4M.2013.6518896

Floridi, L. (2016). On Human Dignity as a Foundation for the Right to Privacy. *Philosophy & Technology*, 307–312. https://doi.org/10.1007/s13347-016-0220-8

Floridi, L. (2018). Soft ethics, the governance of the digital and the General Data Protection Regulation. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2133). https://doi.org/10.1098/rsta.2018.0081

Hardiman, F. B. (2018). Manusia Dalam Prahara Revolusi Digital. *Diskursus - Jurnal Filsafat Dan Teologi Stf Driyarkara*, *17*(2), 177–192. https://doi.org/10.36383/diskursus.v17i2.252

Herdiana, Y., Munawar, Z., & Putri, N. I. (2021). Mitigasi Ancaman Resiko Keamanan Siber. *Jurnal ICT : Information Communication & Technology*, *21*(1), 42–52. https://ejournal.ikmi.ac.id/index.php/jict-ikmi/article/view/305/pdf

Imtiaz, S., Ali, S. H., & Kim, D. J. (2020). E-Commerce Growth in Pakistan: Privacy, Security, and Trust as Potential Issues. *Culinary Science & Hospitality Research*, *26*(2), 10–18. https://doi.org/10.20878/cshr.2020.26.2.002

Peraturan Badan Siber Dan Sandi Negara Nomor 8 Tahun 2020, 1 Bssn 20

(2020).

Kusumastuti, F., Astuti, S. I., Astuti, Y. D., Birowo, M. A., Hartanti, L. E. P., Amanda, N. M. R., & Kurnia, N. (2021). *ETIS BERMEDIA DIGITAL*. Kementerian Komunikasi dan Informatika. http://literasidigital.id/books/modul-etis-bermedia-digital/

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659–671. https://doi.org/10.1016/j.bushor.2021.02.022

Luke, A. (2018). Digital Ethics Now. *Language and Literacy*, *20*(3), 185–198. https://doi.org/10.20360/langandlit29416

Mago, N. (2014). INTELLIGENT CYBER DEFENSE SYSTEM (ICDS): HYBRID APPROACH TO DETECT AND DEFENSE AGAINST CYBER CRIME. *Apeejay Journal of Computer Science And Applications*, *2*, 54–60. https://acfa.apeejay.edu/docs/volumes/journal-2014/paper-09.pdf

Mohamed, H., & Ali, H. (2020). Finding Solutions to Cybersecurity Challenges in the Digital Economy. *IGI Global*, 80–96. https://doi.org/10.4018/978-1-7998-4390-0.ch005

Mujeeb-ur-Rehman, Lakhan, A., Hussain, Z., Khoso, F. H., & Arain, A. A. (2021). Cyber Security Intelligence and Ethereum Blockchain Technology for E-commerce. *International Journal of Emerging Trends in Engineering Research*, *9*(7). https://doi.org/https://doi.org/10.30534/ijeter/2021/21972021

Mylrea, M., Gourisetti, S. N. G., & Nicholls, A. (2018). An introduction to buildings cybersecurity framework. *2017 IEEE Symposium Series on Computational Intelligence, SSCI 2017 - Proceedings*, *2018-Janua*, 1–7. https://doi.org/10.1109/SSCI.2017.8285228

Nafi'ah, R. (2020). Pelanggaran Data Dan Pencurian Identitas Pada E-Commerce. *Cyber Security Dan Forensik Digital*, *3*(1), 7–13. https://doi.org/10.14421/csecurity.2020.3.1.1980

Naseer, H., Maynard, S. B., & Desouza, K. C. (2021). Demystifying analytical information processing capability: The case of cybersecurity incident response. *Decision Support Systems*, *143*(December 2020), 113476. https://doi.org/10.1016/j.dss.2020.113476

Norwawi, N. M., Alwi, N. H. M., Ismail, R., Wahid, F., & Alkaenay, N. M. (2014). Promoting Islamic Ethics on Privacy in Digital Social Network for User Data Protection and Trust. *'Ulūm Islāmiyyah Journal*, *13*(Special Edition), 115–127. https://doi.org/10.12816/0012632

Pilliang, Y. (2012). MASYARAKAT INFORMASI DAN DIGITAL: Teknologi Informasi dan Perubahan Sosial. *Jurnal Sosioteknologi*, *11*(27), 143–155.



Rachman, M. F., & Susan, N. (2021). Modal Sosial Masyarakat Digital dalam Diskursus Keamanan Siber. *Jurnal Indonesia Maju*, *1*, 1–11. https://www.jurnalim.id/index.php/jp/article/view/6

Rahmawati, I. (2017). Analisis manajemen risiko ancaman kejahatan siber dalam peningkatan cyber defense. *Jurnal Pertahanan & Bela Negara*, *Vol.7*(No.2), 51–66.

Siber, P. (2020). *Statistik Jumlah Laporan Polisi yang dibuat masyarakat*. https://www.patrolisiber.id/statistic

Véliz, C. (2019). Three things digital ethics can learn from medical ethics. *Nature Electronics*, *2*(8), 316–318. https://doi.org/10.1038/s41928-019-0294-2

Widiantari, M. M. (2021). URGENSI CYBER LAW DALAM KEHIDUPAN MASYARAKAT INDONESIA DI ERA DIGITAL. *Proceeding of Conference on Law and Social Studies*.



THE PHENOMENON OF ONLINE CONSUMER DATA SECURITY IN ISLAMIC VALUE-BASED DIGITAL ETHIC

ORIGINALITY REPORT

5%	1%	0%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to UIN Ar-Raniry Student Paper	4%
2	www.ssoar.info Internet Source	1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		