Received: 30 October 2021; Revised: 21 March 2022; Accepted: 21 May 2022

ISLAMIC-BASED DIGITAL ETHICS: THE PHENOMENON OF ONLINE CONSUMER DATA SECURITY

Afriyan Arya Saputra[1*]
Muhammad Iqbal Fasa[2]
Diana Ambarwati[3]
[1,3]Institut Agama Islam Negeri Metro Lampung
[2]Universitas Islam Negeri Raden Intan Lampung
[*]*Corresponding Email: afriyanaryasaputra@gmail.com*

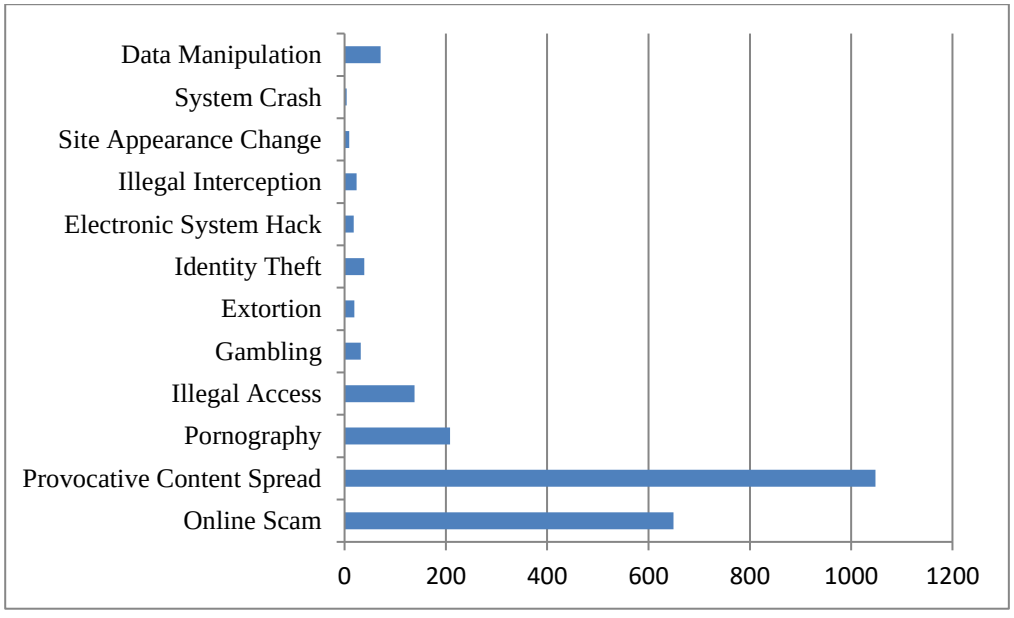
ABSTRACT - This paper seeks to explain the problem of widespread consumer data theft and the significance of online consumer data privacy in a review of Islamic values-based digital ethics. This research employs a qualitative approach by reviewing a variety of books, journals, papers, and other reputable sources, which are then examined using content analytic tools. The findings of this research indicate that first and foremost, effective cybersecurity will secure customer data. Second, ethical conduct derived from Islamic beliefs will be able to deter criminal activity and data breaches against consumers. Data privacy is a fundamental right that must be maintained collectively, according to Islam. The key to combating crime and breaches in the digital environment is hence the precautionary principle of stakeholders.
Keywords: Cyber Security, Digital Space, Digital Ethics, Islamic Value

ABSTRAK – Etika Digital Berbasis Islam: Fenomena Keamanan Data Konsumen Online. *Penelitian ini bertujuan untuk menjelaskan fenomena maraknya pencurian data konsumen serta melihat posisi penting privasi data konsumen online dalam tinjauan etika digital berbasis nilai Islam. Penelitian ini menggunakan metode kualitatif, dengan menelaah berbagai literatur baik buku, jurnal, laporan dan sumber reliable lainnya yang kemudian dianalisis menggunakan teknik content analysis. Hasil penelitian ini menemukan bahwa, pertama, keamanan siber yang baik akan mampu melindungi data konsumen. kedua, perilaku etis yang bersumber dari nilai Islam akan mampu mencegah kejahatan dan pelanggaran data konsumen. Ketiga, dalam Islam data privasi merupakan hak dasar yang harus dihormati secara bersama-sama. Untuk itu prinsip kehati-hatian daripara stakeholder menjadi kunci melawan kajahatan dan pelanggaran diruang digital.*
Kata Kunci: *Keamanan Siber, Ruang Digital, Etika Digital, Nilai Islam*

INTRODUCTION

E-commerce platforms in Indonesia have the third-highest number of users in the world, and are expanding rapidly. The five largest e-commerce companies in Indonesia have incorporated fundamental BCF elements for account verification and transaction processing. In this instance, e-commerce continues to prioritize consumer data security. Despite this, cybersecurity is not a concern for the expanding e-commerce businesses. E-commerce places greater emphasis on the business's profitability and market expansion. One businessman disclosed that selling data is more lucrative than buying and selling items. They sell consumer information, such as residence addresses, e-mail addresses, age and gender, frequently purchased products, and mobile phone contacts. A follow-up strategy derived from the acquired customer data can be utilized for business partner presentations. With the intention of attracting investors who will finance the expansion of their enterprises.

According to the Bulletin APJII (2021), there are even programs that communicate user data to third parties. The shared information includes purchase information, location, contact lists, user content, diagnostics, and financial data. This phenomenon is a widespread practice exemplified by Instagram and Facebook, which care more about gathering user data than securing it.



Graph 1. Cybercrime Trends in Indonesia
(Source: Siber, 2020)

Currently, the threat to the security of online consumer data is growing more concerning. At least two cases have been identified: in mid-2020, Startexmislead accounts offered 12,957,573 data on the Raid Forum of the dark web, and in mid-2021, the owner of the Kotz account sold 279 million Indonesian population data on the same forum. Personal information is susceptible to theft in both instances. In fact, according to Cyber Patrol data, there were 2,259 public reports of cybercrimes from January to December of 2020 (see Graph 1). This demonstrates how dangerous the issue of cyberspace data security is to its users. According to Mohamed and Ali's (2020) research, cybersecurity can be enhanced by increasing surveillance and adopting innovative technologies.

Previous research on online consumer data security has primarily focused on two aspects. First, research on the function 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 research on cyber security framework mitigation and development (Amatullah et al., 2020; Mylrea et al., 2018; Nafi'ah, 2020). The majority of research on these two topics does not address digital ethics based on Islamic values. Where cyberspace interactions are closely tied to behavioral values.

Therefore, this study will describe the phenomenon of consumer data security from the perspective of digital ethics based on Islamic values. Through a review of digital ethics based on Islamic values, this paper will complete the understanding of cybersecurity. This study describes in detail a review of the impact of digital ethics based on Islamic values on the data security of online shoppers.

The paper’s remaining sections are structured as follows: In section two, certain ideas and works of literature on consumer data, cyber security, and Islamic value-based digital ethics are examined. The third section focuses on data and research methodology, whilst the fourth section offers and examines empirical findings. Conclusions and suggestions for further study are provided in the last section.

LITERATURE REVIEW

Consumer Data: Privacy to Protect

The term "data" refers to accurate and genuine information or material that may serve as the foundation for an investigation (and subsequent analysis and conclusions) (KBBI, 2020). In addition, the government regulation Number 82/2012 explains that "personal data" refers to particular individual data that is stored, maintained, and kept truthful while also protecting its confidentially. Personal data encompasses a person's communications (history) and information about such individual.

According to Voigt and Bussche (2017), data is all information that is kept either electronically or in the form of signals or indicators. Data is deemed personal if it pertains to an individual who can be directly or indirectly identified using an identifier. In most cases, the term "identifier" will refer to one or more characteristics that are expressions of a person's physical, physiological, psychological, genetic, economic, cultural, or social identity. Some examples of such characteristics include a person's name, address, email address, date of birth, identification number, location, and online identifiers (such as their IP address or cookies).

Article 26 of the ITE Law confirms that the protection of personal data is a component of the privacy rights, which include the right to enjoy a private life and be free from interference, the right to be able to communicate with others without being spied upon, and the right to monitor access to information about a person's personal life and data (ITE Law, 2008).

One type of cyber threat is a breach of personally identifiable information. In the digital environment, criminals searching for a means to steal someone is identity frequently target multiple pieces of personal information (Wheatley et al., 2016). According to Rebovich (2021), identity theft is defined as making use of the personal identification of another individual without first obtaining permission from that individual's rightful owner. This leads to the conclusion that as more people become interested in the digital world, there will be a greater demand for data and a greater number of people committing the crime of data theft.

Cyber Security: Ensure Data Security

Cybersecurity terminology is still relatively new in the literature. However, as cybersecurity concerns grew, it quickly expanded and eventually became a major issue in every country. According to Branch (2021), cybersecurity terminology began to be addressed throughout the world in the mid-1990s, when there was a "information war." The word refers to an assault and defense operation on computer networks that targets classified material.

There are at least some definitions of cybersecurity in the extant literature. According to Dixit and Silakari (2021) and Mago (2014), cybersecurity is the protection of hardware, software, and data included in an internet-connected system from unauthorized access and cyber-attacks. Meanwhile, Sarker et al (2020) defined cyber security as "the protection of information technology systems and applications against threats, attacks, and cyber risks." Furthermore, cyber security focuses on computer network security from assaults or other forms of intruders, data privacy security information, operational security consisting of policies, processes, and the protection of data that is an asset.

According to Corallo et al. (2021), cyber security is not limited to information technology (IT) systems since it affects the entire ecosystem of operational technology (OT), which interacts with the physical world. Rachman & Susan (2021) argued that cyber security is not confined to concerns associated with technology issues, but also includes the threat of radical awareness inside the internet community. Therefore, cybersecurity can be viewed as the development of mechanisms — both in the physical and digital worlds — to defend against cyber threats and attacks that target data confidentiality.

Discussions about cyber security are increasing in tandem with the growing number of internet users. Because the use of the internet in a country creates potential for cyber-attacks, resources or a system are required to secure cyberspace; this system is referred to as cybersecurity (Craigen et al., 2014). Building a cyber security system necessitates knowledge of security protocols. The cyber security system is deemed capable of preventing cyberattacks or threats through a set of procedures. Similarly, Egloff and Cavelty (2021) highlighted that cyber security systems must be supported by cybersecurity knowledge while conducting attribution assessments, which are the foundation for internet users' security from cyber-attacks.

The Buildings Cybersecurity Framework (BCF) refers to the National Institute of Standards and Technology (NIST) to develop vital infrastructure and consists of five main elements: identify, protect, detect, respond, and recover. Mylrea et al. (2018) elaborated: (1) Identify identifies various cybersecurity threats and weaknesses; (2) Protect recommends handling in managing cyber risk; (3) Detection focuses on techniques, policies, and procedures for detecting cyber-attacks; (4) Respond focuses on handling in responding to cybersecurity incidents; and (5) Recover focuses on restoring normal operating services.

Even though there are precise standards for designing a cybersecurity system, cybercrime still exists. In general, cybercrime is committed through exploiting flaws in the cybersecurity system. According to Sharma and Kumar Sharma (2020), the method utilized to begin cybercrimes includes:

1. Cyberstalking is a type of cybercrime in which the criminal follows the victim online. This activity enables offenders to annoy their victims using electronic mail and messaging applications.
2. Cyber assassination is a cybercrime that involves the murder or defamation of a victim using cyber media.
3. Hacking is gaining illegal access. This operation permits hackers to see, copy, and alter data without deleting it.
4. Cracking is an act of cybercrime that aims to destroy data or hardware by leveraging unauthorized access to the victim's device or server.
5. E-mail phishing is a cybercrime that involves the creation of messages with phony sender addresses.
6. SMS bluffing is a cybercrime that involves the use of short message services. The message is a bogus text message issued under a phony identity, which may be a person or a business.
7. Bot networks, a group of interconnected, virus-infected computer systems. With the target, the criminal controls the victim's computer.
8. Theft of copyrighted assets, company secrets, and contamination of company trademarks constitute Cerebral Property Crime.
9. Cyber crouching is the registration, trading, and use of domain names on the internet while exploiting the victim's trademark. The purpose of this action is to profit from the trademark.
10. Cyberterrorism is an instance of cybercrime. Even the offenders engage in cyber warfare by committing acts of aggression through the internet with the purpose of causing large-scale disruptions.

11. Data theft (identity) is the fraudulent act of stealing other people's information. Typically, data theft occurs on unprotected websites or social media platforms, and it is also widely disseminated via email promos that entice recipients to click on malicious links.

The prevalence of cyber-attacks such as data theft demonstrates the significance of ensuring the integrity of cybersecurity systems. Because all Internet users have the right to privacy and are free from societal pressure (Burgoon, 1982) or being spied on by any party, it would be unethical for any organization to conduct surveillance on Internet users (Widiantari, 2021). For this reason, with reference to regulation of *Badan Siber dan Sandi Negara* No. 8/2020, electronic system operators (both public and private) must maintain the security of information management. Thus, electronic system operators are expected to develop cyber security that prioritizes cyber security principles to protect privacy and consumer rights, such as the use of on-time passwords, personal identification numbers (PIN), end-to-end data exchange, and enhanced system surveillance (Amatullah et al., 2020), and the implementation of advanced encryption techniques (Nafi'ah, 2020).

Islamic Value-Based Digital Ethics

The study of digital ethics is a contemporary topic that refers to digital notions that are regarded as unusual. Existing academic literature has a few of definitions of digital ethics, the vast majority of which are remarkably similar. Luke (2018) defines digital ethics as the ethical principles that govern internet interactions. Schoentgen and Wilkinson (2021) feel that a person's values and beliefs serve as the basis for the formulation and implementation of ethical procedures when it comes to internet ethics. According to Kusumstuti et al. (2021), internet ethics is concerned with acts and all interactions based on conscious, responsible, honest, and virtuous behavior that enhances the quality of human life.

The three definitions presented above highlight the fact that digital ethics is concerned with activities and interactions that are carried out in cyberspace. The manner in which actions and interactions take place in cyberspace reveals three types of relationships: those between individuals, those between communities, and those between communities and individuals. These three types of relationships all live out a life model through the utilization of cyberspace as a method of mediation (Pilliang, 2012).

The use of moral principles in online interactions is an absolute requirement that cannot be avoided. A lack of ethical conduct in cyberspace can lead to mistrust, hostility, conflict, and the misuse of digital tools, all of which can result in significant financial losses (Véliz, 2019). Users of the internet who behave ethically can avoid these negative outcomes. According to Floridi (2016), ethics are able to control humans to act more morally, and they are also able to build value in relationships and interactions so that they are more valued. Additionally, ethics are able to control individuals to act more morally than they would otherwise (Kamri, Ramlan, & Ibrahim, 2014). In addition, a person's belief in his faith can help establish ethical behavior in online.

The value of Islamic teachings, as Chaudhary (2020) argues, establishes the individual as a moral subject who actualizes his personal activity with full awareness and prioritizes moral aspects and responsibility. In other words, the individual is a moral agent. This moral conduct derives its justification from Islamic precepts (Ibrahim & Kamri, 2013). Within the framework of Islamic thought, morality occupies a place of utmost importance. In Islam, ethical conduct is based on the following five principles: (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; Ibrahim & Kamri, 2016, 2017).

These principles serve as the foundation for constructing values that are derived from the Qur'an and hadith. In addition to this, the actualization of Islamic beliefs will lead to ethical behavior in virtual spaces. In this context, the value of monotheism is connected to things that are worthy of being worshipped. This indicates that every action or behavior is designed as a step toward realizing monotheism to the extent that Allah SWT is concerned. This idea illuminates the significance of monotheism, which is present in each and every facet of human existence. In accordance with the saying of Allah Ta'ala in the al-Qur'an:

> *"That is, for indeed Allah, He is the real one, and whatever they call on besides Allah is falsehood. And verily Allah, He is the Highest, the Greatest."* (Surah Luqman: 30)

The concept of equilibrium value refers to being honest, straight-forward, and fair, as well as equalizing objects in terms of their size and value. According to what Allah Ta'ala says, the advice to be fair is as follows:

> *"Indeed, Allah commands (you) to do justice and do good, to give help to relatives, and He forbids (to do) abominable acts, evil deeds, and enmity. He teaches you so that you can learn a lesson."* (Surat an-Nahl: 90)

In spite of the fact that he possesses free choice in the manner in which he chooses to express his life activities, the value of being a caliph means that there are constraints on human behavior. Humans, in their role as caliphs, are obligated to flourish economically and to disseminate wealth throughout the world and the earth by working together and assisting one another (Surah An-Nahl: 90). Through the completion of this work, humans are positioned as components of a very broad unity of creation. As the saying of Allah Ta'ala:

> *"And it is He who has made you caliphs on earth and has raised (degrees) some of you above others, to test you for the (bounty) He has given you. Verily, your Lord is swift in punishing, and indeed, He is Most Forgiving, Most Merciful."* (Surat al-An'am: 165)

The importance of virtue, or an ethical concept, is that it encourages the dissemination of usefulness. The conduct of desiring to be of service to others is an indication of how the Ihsan value is put into practice. In relation to the importance of virtuous behavior, the Word of God is as follows:

> *"O you who believe! Bow, prostrate, and worship your Lord, and do good, that you may prosper."* (Surat al-Hajj: 77)

The value of accountability, in which all activities will be held accountable both in this world (during life) and in the afterlife. Regarding its status as the Word of God:

> *"O you who believe! Fear Allah and let everyone pay attention to what he has done for tomorrow (hereafter), and fear Allah. Indeed, Allah is All-Aware of what you do."* (Surat al-Hashr: 18)

RESEARCH METHOD

This study employs a qualitative methodology, which is based on non-numerical data or data in the form of text and images, and data filtering is performed to derive interpretations from the literature review (Creswell, 2014). To gain a holistic grasp of reality, a qualitative technique is employed to describe occurrences. To comprehend the phenomena of online consumer data theft, this study employs literary studies as an analytical tool, in the form of books, journals, and other credible sources. The study's obtained data were then categorized based on the specified research questions. The data in this study are given in a narrative-descriptive format and examined utilizing a content analysis technique. Referring to Hsieh and Shannon (2005), content analysis is utilized to understand classified text data in order to derive a conclusion.

RESULTS AND DISCUSSION

Result

The theft and breach of personal data undeniable fact

Before a consumer is granted access to an application, they are always needed to consent to the developer's privacy policies. It is required to secure this clearance in order to guarantee continued consumer access. If this is not the case, then you cannot utilize the application. The agreement will grant access permissions to the program developer, allowing the developer to analyze the personal information of users who are logged into the device. Because we want all private information and access data stored on our devices to be readily identifiable by the developers who operate on them. This indicates the possibility of illegal use of personal information.

According to the author, this is a crucial factor in the theft of client data. Users of the Internet who get unauthorized access are the offenders of the crime of data theft. According to the most recent Databoks Report 2020, 105,2 million e-commerce user records were compromised. Usernames, email addresses, and passwords for online accounts were among the information that was compromised. The table below illustrates the high rate of data theft that will occur among online marketplace clients in Indonesia in 2020.

Table 1. Number of E-Commerce Data Theft

Name	Lots of Data Stolen
Tokopedia	91 Million
Bukalapak	13 Million
Bhinneka	1,2 Million

(Source: Databoks, 2020)

The material offered above illustrates that unauthorized access to and use of a person's personal data is not a myth, but rather an undeniable fact. The increase in data theft in Indonesia, as reported by Komalawati et al. (2021), is a result of weak cyber security, which makes it simple to steal consumer data. Therefore, preemptive measures should be taken to strengthen cyber security in order to protect the privacy of customer data. According to Lee (2021), it is necessary to pay attention to the cyber ecosystem (stakeholders), the evaluation of cyberinfrastructure (such as users, workforce, and technology), the assessment of cyber risks (such as identification of devices, vulnerabilities, threats, and cyber-attacks), and cybersecurity activities in order to maximize the function of cybersecurity in protecting data privacy and digital assets. According to Naseer et al. (2021), innovation in cybersecurity must focus on the development of apps that integrate threat intelligence data, automation of threat detection, forensic analysis, algorithm application, and the research of internet users.

There is an urgent requirement for the development of cyber security in order to ensure the privacy and reliability of data. Taking into account the fact that cyber threats originate from a variety of actors, including those working for foreign intelligence agencies, actors who have become disillusioned with their work, investigators, extremist organizations, hacker activities (hacktivist), and activities from organized crime groups. This risk also develops as a result of criminal actions conducted online, which target information and data security systems that are connected to the internet network. These criminal activities can even pose a threat to the military operations of a country (Rahmawati, 2017). These dangers will, without a doubt, have an impact on both real and virtual society.

Technology advancements can be used to fortify internet defenses. According to Herdiana et al., (2021), the deployment of cutting-edge technology and algorithm modifications throughout the system will have an effect on the security system's precision. This includes the use of technologies such as the internet of things (IoT), blockchain, artificial intelligence (AI), avatar-based

management techniques, and others. According to Mujeeb-ur-Rehman et al. (2021), the implementation of rigorous privacy security cycle stages is appropriate for preserving the data privacy of internet users (clients, merchants, and online transaction systems) by using advanced technology as cybersecurity. This can be accomplished by utilizing advanced technology such as cybersecurity. The protection of Internet users' personal information is a critical issue.

Cybersecurity, which is merely a method in the process of developing privacy policies for internet users, has been shown to be unsuccessful, despite the fact that it is necessary to secure the data of consumers (Ebert et al., 2020). For this reason, in order to preserve privacy, in addition to prioritizing cyber security principles, the implementation of artificial intelligence (AI) as a cyber security technology is required (Herdiana et al., 2021). On the other hand, socialization is also required to ensure that internet users receive education pertaining to cyber security (Rahman et al., 2020). According to de Bruijn and Janssen (2017), individual elements, such as internet users, need to also take action to protect the privacy of their data. The mentality of internet users is the most important factor in determining the choices they make when using the internet. Consumers, and particularly those customers who conduct business online, hold a crucial role in ensuring the safety of their own personal information against online risks such as data theft.

Factors Supporting Consumer Privacy Data Breach

The likelihood of cyber threats is directly proportional to internet usage. The potential for damage resulting from cyberattacks is growing. This is due to the misuse of technological advancements by those who conduct cyber attacks. This means that people who utilize unlawful access also apply technology to research data theft vulnerabilities. However, similar to the previous section, technological advancements can also be used to combat cybercrime.

The development of continually new technology, infrastructure, and method models is one of the ways that efforts are being made to increase cybersecurity. A more significant cyber danger has been recognized, and this program is a response to that threat. There is a widespread perception that the current methods of cybersecurity are inadequate to secure the privacy of internet users in an effective manner. On the other hand, technology integration with network changes such as 5G, IoT (Dawson et al., 2021), and AI (Djenna et al., 2021) is

thought to be capable of building a comprehensive, strategic, and reliable cyberinfrastructure in dealing with cyber threats on a large exploitative scale.

In addition to the role that technology plays, users of the internet also have a duty to play in the protection of the confidentiality of their data. Choo (2011) recommended stakeholders such as users, organizations, governments, and research institutions that rely on the internet to continue innovating in order to combat cyber dangers such as data theft after seeing the fast expanding cyber threat landscape. Therefore, the possibility of people who utilize the internet cannot be discounted.

The decisions that internet users make in response to comprehending the dangers of cyberspace are influenced by digital ethics. According to Floridi (2018), providing an explanation of ethical behavior in cyberspace helps ensure that users are aware of potential dangers, prioritize the precautionary principle, and decrease risks due to the fact that ethically compliant users can decline data requests from malevolent access. A cybersecurity landscape in which internet users are aware of each other's privacy is being pursued, and one of the most important components in achieving this goal is ethical behavior. Each individual is solely responsible for their own level of privacy protection and access to data for evaluation.

The previous explanation divides internet users into three groups. First, consider internet users as market players whose primary activities are purchasing and selling. Second, internet users are market employees who must control the security of their customer data. Third, internet users steal data. Each of these three types of internet users has its own set of ethical guidelines. Users of the Marketplace have the ability to approve or deny requests for damaging access, which necessitates user attentiveness. While program developers can be held more accountable for protecting user data. Application developers' ethical behavior may also include the use of passwords and PINs sent directly to the authorized data owner's contact or e-mail address, as well as the improvement of system surveillance and the deployment of advanced encryption techniques. Meanwhile, unethical programmers and internet users who commit data theft are more concerned with the damage they cause than with personal or collective benefits.

Discussion

Who is responsible for cybersecurity?

Cybersecurity should be prioritized in the safeguarding of customer information. However, in Indonesia, this position has not been very effective. This is due to the fact that there are application developers that are supposed to preserve consumer data privacy but simultaneously engage in the practice of buying and selling such data for financial advantage. This predicament is the result of application developers buying and selling client data. Furthermore, a considerable number of people who embrace growing degrees of technological skill are contributing to the deterioration of this condition. Therefore, the protection of consumers' personal information is an extremely essential issue that must be managed properly.

To prepare for this, it is essential to use technology in the process of constructing cyber security, as this will have an effect on the reliability of cyber security in general (Dawson et al., 2021; Djenna et al., 2021; Herdiana et al., 2021). Building a dignified cybersecurity landscape requires prioritizing the enhancement of the privacy and safety of consumer data. The government is wielding its power like an iron fist to establish stringent regulations that would strengthen cyber security. The existing restrictions solely focus on marketplace application developers buying and selling user data. There is a need for regulations so as not to perpetuate the misconception that cyberspace is extremely unrestricted and therefore poses no threat to users' privacy.

Furthermore, it is vital for application developers and other actors in the digital world to conduct themselves ethically. The perpetrators' moral commitment will have a good impact on the climate of the digital environment. Ethical behavior is an internal state that is entirely under the control of the individual, both as a consumer and as a moral internet user. An ethical conduct will provide certain frames or borders that are good, terrible, safe, and damaging in order to divert criminals away from committing crimes and violating consumers' privacy data.

On the other hand, the responsibility that the user has for maintaining the confidentiality of his data ought to be reinforced when unauthorized access permissions are being requested. Despite the fact that the application developers continue to abuse the system that allows them to grant access permissions, the system continues to function as intended. This is a cause for

concern, and in the APJII Bulletin Edition 84, it is even urged that in the future, users of any program must prioritize prudence and pay close attention to any information that is provided to the application developer.

Consequently, maintaining the security of consumer data privacy is a shared obligation. It is not only the government's role as a stakeholder in this topic, but also the responsibility of every internet user as a service provider, application developer, and service user.

The precautionary principle can prevent privacy data breaches and crimes in cyberspace

The landscape of cybersecurity is shaped by a variety of factors, including the infrastructure and technology used by service providers and application developers, as well as the ethical behavior of each individual internet user. When it comes to maintaining behavior in cyberspace, ethics is crucial. The Islamic principle instructing followers to use cyberspace in a way that does not cause harm to themselves or others demonstrates the critical need for an Islamic-based digital ethics system.

Putting forward the values found in Islamic business ethics will undoubtedly provide comfort to all internet users. These values include the concepts of monotheism, justice and balance, freedom and freewill (human nature as the caliph of Allah SWT); benevolence or *Ihsan* (beneficial actions for others); and responsibility. Through these concepts, internet users can reflect on the importance of worship in their cyberspace interactions. To put it another way, the worth of good and bad behavior must be considered. Because cyberspace users do not want their data privacy to be violated by anyone. As a result, cyberspace, which is interpreted as a space for free expression, must also consider the freedom of others.

The preceding demonstrates that the assurance of a feeling of safety while interacting in cyberspace can be initiated through the morally upstanding conduct of each individual member of a cyber society. Respect for an individual's right to solitude is a fundamental tenet of Islam (Norwawi et al., 2014; Akmal, Musa, & Ibrahim, 2020). This provides further evidence that, in accordance with digital ethics founded on Islamic values, the concentration of power is distributed among individuals in proportion to the portions they control. First, there is an improvement in the infrastructure and technology of cybersecurity service providers and developers. Second, customers who engage

in financial transactions (also known as internet users) place a premium on their moral conduct while online.

Digital ethics serves as a moral compass in cyberspace. Consumers (users) of marketplace applications are the most vulnerable type of internet user. While concerned with digital ethics based on Islamic values, online consumers are viewed as internet users with the authority to maintain the security and privacy of their data. When online consumers are aware of cyber threats, they can use the precautionary principle (Floridi, 2018) to make decisions about the transparency of their data. Furthermore, the precautionary principle is an important pillar in ensuring the security and privacy of consumer data. Customers can be aware of their private areas under this principle. As well as the authority to make decisions on the review of his personal data. Where these efforts on occasion become supporters for the formation of a cyber security landscape.

Consumer data security perspective of Islamic value-based digital ethics

The state of internet users is becoming increasingly concerning. According to Hardiman (2018), the cyber community (homo digitalis) acts very brutally in cyberspace when using the internet network. According to Choiriyati & Windarsih (2019), such a situation demonstrates the need for ethical construction that is more knowledge-based in nature and is derived from religious values. In this regard, digital ethics based on Islamic values should be conceptually transformed to be more applicable. So that ethical behavior formed in cyberspace is consistent with the instructions contained in internet users' religious beliefs. Furthermore, Chaudhary (2020) explains how the value of Islam can actualize the responsible behavior of its adherents. Where Islamic ethics helps to build a civilized and moral life In the digital space, ethical values based on Islamic values are critical for creating a business climate that adheres to values and ethics (Ambarwati, 2013; Umuri & Ibrahim, 2021).

People who believe in their religious values are more likely to use the internet, and the fact that behavior and interactions are highly valued in Islam ranks first. Furthermore, awareness of privacy among internet users and application developers regarding the safety of data in cyberspace is something that must be taken into account, as self-respect is closely linked to privacy in Islam (Norwawi et al., 2014). The right to privacy is fundamental, and all parties involved are obligated to protect it. In Islam, the act of granting permission is

inextricably linked to the concept of personal privacy. In the Qur'an, Allah SWT says:

> *"27. O you who believe, do not enter houses other than your own until you are sure to welcome and greet their occupants. That's what's best for you; maybe you will be reminded. 28. And if you find no one in it, do not enter it until you are given permission... 29. There is nothing wrong with you entering uninhabited houses in which there is comfort for you..."* (Surat an-Nur: 27-29)

The preceding paragraph underlines the need of consent in privacy. According to Asad (2017a), the content in verse 27 has a protective function for persons against the danger of slander. Furthermore, Asad noticed in the letter that the content of the prohibition's meaning is a valuable foundation for the idea that one's privacy should not be invaded. Asad interprets the 28th verse to mean that permission is granted to someone who is the proper owner or person in charge of privacy. Asad says in his reading of the 29th verse that areas that can be approached without permission are buildings such as public utilities, including historic buildings that have collapsed. In this scenario, though, the researcher perceives cyberspace as a private "place" for someone. Aside from the advice to acquire permission, there is also a restriction on suspecting, spying on, and disclosing information belonging to others (slander). According to Allah SWT's Word:

"O you who believe, stay away from many [negative] prejudices…" (Surat al-Hujurat: 12)

The prejudice mentioned in Surah Al-Hujurat verse 12 is a type of bias that has the ability to produce undue distrust of others (Asad, 2017b). The above Qur'anic verses stress that Islam is particularly concerned about privacy and security issues where the principle of secrecy must be respected. To protect data privacy in cyberspace, ethical behavior is required. According to Faisal et al. (2013), service providers and application developers must pay attention to privacy issues, while consumers should play a part in regulating privacy by prioritizing Islamic principles. This is equally true for the security of online consumer data. According to Imtiaz et al (2020), e-commerce that does not prioritize consumer data security would lose consumer trust. Furthermore, Islam places a premium on the protection of internet customer data privacy.

Cyberspace, being an interactive domain, should be handled with caution. To avoid negative outcomes, the ethical behavior of every internet user who uses cyberspace must be accomplished collectively. Islamic morals that are essential for its members are particularly important when it comes to internet security and privacy. The Islamic viewpoint on unauthorized access is incorrect. The license granted for data privacy access should not be abused. The use of Islamic values in consumer data security is everyone's obligation to preserve each other's privacy on the internet.

CONCLUSION

Based on the discussion, it is possible to infer that digital ethics founded on Islamic values can serve as a means of moral development for internet users, particularly consumers who conduct online transactions. Through the promotion of Islamic values-based ethics, cyber security can be established. Consumers gain the independent authority to make decisions to secure their data as a result of the instillation of these principles. Meanwhile, other internet users can be held more accountable for their online behavior. The ruling, reinforced by ethical cyberspace behavior, demonstrates that cybersecurity is a problem that must be addressed collectively.

In Islam, privacy is associated with self-respect. Privacy is a fundamental human right that must be respected both individually and collectively. To protect one's privacy in the digital world against violations and crimes, the principle of prudence should be prioritized in transactions and interactions. Similarly, developers should respect and protect consumer privacy data, rather than exploiting it for personal advantage.

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

Akmal, R., Musa, A., & Ibrahim, A. (2020). Pengaruh Religiusitas terhadap Perilaku Etika Bisnis Islam Pedagang Pasar Tradisional di Kota Banda Aceh. *Journal of Sharia Economics*, *1*(1), 1-21.

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

APJII, T. (2021). Buletin APJII. *APJII*. https://apjii.or.id/downfile/file/BULETINAPJIIEDISI84April2021.pdf

Asad, M. (2017a). *The Message of The Quran: Tafsir Al-Quran Bagi Orang-orang yang Berpikir* (A. Muhammad (ed.); Vol. 2). PT Mizan Pustaka.

Asad, M. (2017b). *The Message of The Quran: Tafsir Al-Quran Bagi Orang-orang yang Berpikir* (A. Muhammad (ed.); Vol. 3). PT Mizan Pustaka.

Branch, J. (2021). What's in a Name? Metaphors and Cybersecurity. *International Organization*, *75*(1), 39–70. https://doi.org/10.1017/S002081832000051X

Peraturan Badan Siber dan Sandi Negara Nomor 8, (2020). https://peraturan.bpk.go.id/Home/Download/167483/Peraturan BSSN Nomor 8 Tahun 2020.pdf

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

de Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7. https://doi.org/10.1016/j.giq.2017.02.007

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

Diana Ambarwati. (2013). Etika Bisnis Yusuf Al-Qaradhawi (Upaya Membangun Kesadaran Bisnis Beretika). *Adzkiya: Jurnal Hukum Dan Ekonomi Syariah*.

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

Ebert, N., Ackermann, K. A., & Heinrich, P. (2020). Does Context in Privacy Communication Really Matter? A- A Survey on Consumer Concerns and Preferences. *Conference on Human Factors in Computing Systems - Proceedings*, 1–11. https://doi.org/10.1145/3313831.3376575

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

Hsieh, H.-F., & Shannon, S. E. (2005). Three Approaches to Qualitative Content Analysis. *Qualitative Health Research*, *15*(9), 1277–1288. https://doi.org/10.1177/1049732305276687

Ibrahim, A., & Kamri, N. A. (2013, 27-28 November). *Measuring the Islamic Work Ethics: An Alternative Approach.* Paper presented at the International Convention on Islamic Management, Kuala Lumpur, Malaysia.

Ibrahim, A., & Kamri, N. A. (2016). The Commitment to Islamic Work Ethics among Islamic Banking's Employees in Aceh *Shariah Journal*, *24*(1).

Ibrahim, A., & Kamri, N. A. (2017). The Ethical Practices of Islamic Banking: An Analysis from Customer Satisfaction Perspective. *MIQOT: Jurnal Ilmu-ilmu Keislaman*, *41*(1).

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

Kamri, N. A., Ramlan, S. F., & Ibrahim, A. (2014). Qur'anic Work Ethics. *Journal of Usuluddin*, *40*(-), 135-172.

KBBI. (2020). *Kamus Besar Bahasa Indonesia (KBBI) Kamus versi online/daring*. Kemendikbud.

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

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393

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

Rebovich, D. (2021). The Changing Face of Financial Crime: New Technologies, New Offenders, New Victims, and New Strategies for Prevention and Control. In *Victims and Offenders*. https://doi.org/10.1080/15564886.2021.1876196

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data*, *7*(1), 41. https://doi.org/10.1186/s40537-020-00318-5

Schoentgen, A., & Wilkinson, L. (2021). Ethical issues in digital technologies. *International Telecommunications Society (ITS)*, *23*. http://hdl.handle.net/10419/238052

Sharma, S., & Kumar Sharma, V. (2020). Cyber Crime analysis on Social Media. *BSSS Journal of Computer*. https://doi.org/10.51767/jc1104

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

Umuri, K., & Ibrahim, A. (2021). Analisis Perilaku Pedagang Kaki Lima Menurut Tinjauan Etika Bisnis Islam. *Jurnal Iqtisaduna*, *6*(2), 187-197.

https://doi.org/10.24252/iqtisaduna.v6i2.17511

UU ITE. (2008). Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Cell*.

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

Voigt, P., & von dem Bussche, A. (2017). Enforcement and Fines Under the GDPR. In *The EU General Data Protection Regulation (GDPR)*. https://doi.org/10.1007/978-3-319-57959-7_7

Wheatley, S., Maillart, T., & Sornette, D. (2016). The extreme risk of personal data breaches and the erosion of privacy. *European Physical Journal B*. https://doi.org/10.1140/epjb/e2015-60754-4

Widiantari, M. M. (2021). Urgensi Cyber Law dalam Kehidupan Masyarakat Indonesia Di Era Digital. *Proceeding of Conference on Law and Social Studies*.