INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN PROGRESSIVE EDUCATION & DEVELOPMENT

OPEN ACCESS JOURNAL

Vol 11, Issue 3, (2022) E-ISSN: 2226-6348

Cybercrime and its Violation of Digital Platform Security: An Islamic Law Perspective

Khairul Azhar Meerangani
Academy of Contemporary Islamic Studies, Universiti Teknologi MARA Cawangan Melaka

Ahmad Faqih Ibrahim
Faculty of Islamic Knowledge, University of Malacca

Muhammad Yasin Omar Mukhtar
Division of Research, Consultation and Innovation, University of Malacca

Muhammad Hilmi Mat Johar, Adam Badhrulhisham
Faculty of Islamic Knowledge, University of Malacca

Muhammad Asyraf Ahmad Termimi
Ministry of Domestic Trade and Consumer Affairs

To Link this Article: http://dx.doi.org/10.6007/IJARPED/v11-i3/14564 DOI:10.6007/IJARPED/v11-i3/14564

Published Online: 25 August 2022

Abstract

The sophistication of today's technology has seen an increase in the demand for online services involving various matters. Although this has a positive impact, this sophistication is potentially misused by certain parties for criminal purposes. Cybercrime is a modern crime that is increasing along with the enlightenment of communication and information technology. Property theft crimes include hacking, scamming, phishing, forgery of credit cards and bank account cards, and illegal money transfers. Cyber crimes are becoming more prevalent nowadays. Therefore, this study is important in exploring the violation of cybercrime on digital platform security form Islamic law perspective. Thus, this study aims to identify the forms of cybercrime in today's digital platforms and their punishment through Islamic law. The study was conducted qualitatively using literature data such as theses and journals to examine the elements of cybercrime according to Islamic law. The study's findings were analyzed inductively to determine today's cybercrime punishments on digital platforms. The change of criminal background from physical to digital format is a new thing that previous Muslim scholars did not discuss. However, the four basic principles of crime set, namely the concept of digital property, transfer of property, invasion of control, and no doubt allow the perpetrator to be convicted of the crime of theft according to Islamic law if they meet the conditions set. Further field research is proposed to obtain more authentic data related to the violation of cyber crime among digital platform's user.

Keywords: Technology, Cyber Crime, Online Transactions, Fraud, Islamic Law

Introduction

The boom in technology and information nowadays has created various facilities in society's life today. Many things and affairs can be done online quickly and effectively. However, not all users will take advantage of the progress resulting from the development of technology and information. Some users use the cyber medium as a platform to commit crimes and make easy profits by abusing the skills and facilities provided. The seriousness of commercial cybercrime involving the loss of money and property has caused several acts to be enacted in Malaysia to curb such crimes (Maskun, 2014). However, among the property cyber crimes that continue to increase yearly is the cybercrime of fraud. Cybercrime statistics released by CyberSecurityMalaysia show that online fraud cases are the highest cybercrime reported in five years, with a total of 3,921 cases received the previous year compared to 3,257 cases in 2015 (Rabi'atul, 2017). The alarming increase in cybercrime has given rise to government initiatives to raise awareness and encourage positive and ethical use of the internet and computers (Ahmad Suhael, 2017).

The Malaysian Computer Emergency Response Team (MyCERT) is an organization under the Ministry of Science, Technology, and Innovation (MOSTI) that was established in 1997 and acted as a reference center in Malaysia for computer security cases. Now MyCERT operates the Cyber999 computer incident handling and response assistance center and CyberSecurity Malaysia's Malware Research Center. MyCERT works closely with law enforcement agencies such as the Royal Malaysian Police (PDRM), Securities Commission (SC), and Bank Negara Malaysia (BNM) while also working with the Internet Service Providers (ISPs) Computer Security Incident Response Team (CERT) as well as various Computer Security Initiatives around the world (MyCert, 2013). MyCert has released statistics for reports of cyber incidents in Malaysia since 1998. They have divided cyber incidents into nine categories: content-related, cyber harassment, denial of service), fraud, intrusion, intrusion attempt, malicious code, and vulnerability report (Ibid.). The report clearly shows that cybercrime is no longer considered trivial and just a simple misdemeanor but has reached the level of severe criminal behavior in cyberspace.

Literature Review

a) Cyber Crime from Islamic Law Perspective

From a terminology point of view, crime means an act of committing, leaving, or as a cause that can cause harm to humans or others which will be subject to worldly punishment (Zuhrah, 1998). According to jurists, crime is an evil act or behavior done by someone to violate or violate the honor of another person's soul or body on purpose (Zuhayli, 1985). Although each crime appears in a different format and provision of punishment, the primary purpose of each execution of the sentence is the same. It aims to protect the religion, soul, intellect, lineage, honor, lineage, and property of every human being so that it is not arbitrarily violated, oppressed, and expropriated while highlighting the beauty of Islamic Sharia. The crime of stealing is one of the crimes provided with hudud punishment. Theft is taking someone else's property that is carefully guarded silently and secretly to possess (Kasani, 2003).

Based on this definition, four elements make up the crime of theft which are (1) taking other people's property or that which is not one's own, (2) the property taken is carefully guarded, (3) the property is taken silently and secretly and (4) the act of taking property to possess. If one of the four elements mentioned is missing, then the conviction of the crime with hudud law will be transferred to the punishment of takzir. For example, suppose the

property does not belong to another person entirely. In that case, the property is in an open area without supervision or taken on a loan rather than for ownership. Therefore, the conditions for the crime of theft are not met, and the hudud punishment cannot be implemented. Instead, it will be replaced by a reprimand. The phrase 'secretly' here indicates usurpation and breach of trust are not included in this term. This is because confiscation is done openly, not secretly or secretly, while the breach of trust does indeed have access to the property. Therefore, the perpetrators of these two crimes will not be convicted and will be sentenced to the limit of theft (Paizah, 2008).

Qudamah (1997) states that the jurists have agreed on the punishment of amputation of the hands of thieves who have been convicted of the crime. However, Islam also outlines the punishment of takzir for the crime of theft, especially for the crime of theft that does not meet the conditions of the conviction of the hudud sentence under the method "hudud punishment is dropped due to the existence of suspicion." Takzir is a punishment whose rate is not determined by the Sharia but by a fair Muslim judge with a sentence capable of preventing an individual from committing a terrible act. This punishment can be imposed in various forms, such as flogging, exile, imprisonment, fines, and censure. This is because acts like this are immorality that is not included in hudud offenses and will not be subject to expiration.

Therefore, if the hudud punishment is not imposed, this offense must be punished with takzir instead (Mustafa et al., 1992). The government determines the setting of the takzir sentence by considering the effects of the crime committed and the background of the criminal himself. In assessing the impact of this crime, Atrusyani (t.t) stated that the judges need to see the reason for the punishment. If the sentence for the criminal offense is of the type of hudud that is dropped due to certain obstacles, then the punishment of takzir must be set at the highest level. But on the other hand, if it is not of the hudud type, then the prescribed punishment is not necessary to the maximum level. But it is sufficient with the consideration that the government feels is appropriate.

b) Essential Element of Cyber Crime

The element of the location of the property storage plays a vital role in determining the penalty limit for trespassing on the property. Various aspects must be considered before deciding that the property is under perfect control or vulnerable to any invasion by irresponsible parties. In determining this principle, the jurists have assessed the conditions that need to be taken into account to ensure that trespassing on the property qualifies for a determinate sentence to be imposed on the perpetrator. Property care is divided into two forms: unique care places such as safes to keep jewelry and money, stables to keep animals, or stores to store goods. The second form refers to a location that does not function as a specific storage place. Still, it includes items that are looked after and supervised by any individual, for example, someone sitting or sleeping in a mosque and putting a bag by his side. This is also included in the concept of care. A suitable storage place means that the property is usually kept in a specific location or similar (Kasani, 2003 & Ansari, 2015), such as money, which is generally saved in a chest, or clothes, which are usually kept in a closet.

This measure refers to local customs (uruf) and the opinion of skilled people. If the property is stolen from a place that is not commonly used to store the property or placed in the open, the punishment of hand amputation cannot be carried out on the thief. So, based on the stipulation, most jurists believe that the hand of a thief who steals property that is not guarded or controlled will not be cut off. In addition, damage to the storage building,

permission to enter the storage place, and the location of the property in the open can also remove the nature of care and control over the property, which, if agreed by the prosecution (judge), then the thief will not be cut his hands. Still, they will only be punished with taking (Qadir, t.t). Therefore, the jurists agree in determining the invasion of al-hirz as a prerequisite for executing the maximum sentence for the crime of theft (Qudamah, 1997).

Thus, the law of the place of storage indeed plays a vital role in determining the position of the theft offender, whether he is sentenced to a determinate sentence or not. This is because one of the main elements in the conviction of the theft crime is the invasion and taking of a property secretly from its strong storage place based on the assessment of local customs with malicious intent (Kasani, 2003). Therefore, every offender who meets the conditions qualifies to be sentenced to a determinate sentence. In general, the jurists divide this treasure storage place into two forms: the storage place (*al-hirz bi nafsihi*) and the storage place that needs a guard (*al-hirz bi al-hafiz*). This determination is made by taking into account the ability of the property storage place to protect the property. This first type of control refers to all areas recognized as property storage locations, and any access to them without permission is prohibited, such as warehouses, unique safes, and vaults. Therefore, trespassing in areas like this will qualify the perpetrator to be punished even without any guardian because the storage location is strong enough to prohibit any form of trespassing. However, the area must first ensure appropriate security levels and standards to prevent any intrusion from irresponsible parties. If the physical location is fragile, its place to store property will fall, and the perpetrator will only be sentenced to takzir.

c) Property Security

The weaknesses and strengths of a storage place are closely related to several elements in determining the position of a property and whether it is classified as a well-kept property. In determining the level of strength and weakness of a place of storage, Mawardi (1994) has established five aspects that need to be given an appropriate assessment, namely the type and value of the property, the structure of the country, the current atmosphere, the judge's background and time. Elements of the class and importance of this property are essential in ensuring the position of care of the property. Property with a high value according to local custom justifies careful and decisive consideration, while property not usually considered valuable by the community does not justify cautious care. In the cyber world, any financial transaction and electronic transfer of information and data has commercial value and has a very high and valuable value in society. This differs from sharing news and general information that can be freely accessed by the public, which is generally not valued as property.

The structure sees countries with large borders and large populations justify immediate care. In contrast, countries with narrow borders and a small number of people who are less mixed with each other explain poor care. In the cyber world, high access to a network requires a high level of security, especially involving property matters, unlike networks that are rarely accessed due to the lack of need for the web. So the story of monitoring the network is also not as strong as a network with high access. Next, the elements of the current atmosphere show a peaceful and peaceful situation justifying poor care due to the lack of attention to the property owned. This is in contrast to the case during the war and the threat of fear which justifies extreme care as a counter-reaction to the dangerous situation. For example, in any cyber attack and peril, a high level of security must be provided for all forms of property owned compared to a calm state without any disturbance and threat.

As for the elements of the judge's background, a judge who is fair and firm towards offenders will justify poor care because of the high trust and confidence in the level of integrity and authority of the judge. This is different from judges who are authoritarian and careless towards offenders who justify a strong group of care in ensuring the safety of their property. Strict laws and authoritative cybercrime enforcers provide a high level of security for where the property is stored in cyberspace. The time factor sees that nighttime requires a level of care because criminals usually go out to commit crimes at that time. This is different from the daytime with the existence of the fantastic group in balancing the evil group, thus justifying the weak level of care due to the indirect monitoring of the incredible group on the property owned by each other. So, based on the stated principles, it is clear that the current uruf factor plays a vital role in determining the strength and weakness of a place where the property is stored. This is important in determining the level of aggression during the prosecution process and in ensuring whether a limited sentence conviction needs to be carried out or the crime will be transferred to takzir punishment due to factors that doubt the strength of the prosecution's argument.

Methodology

This study was conducted qualitatively using data obtained through a literature review. The documentation method highlights literature materials such as scientific books, journals, articles, seminar proceedings, and reports. This literature review is critical because, through this method, the researchers get a clear picture of the principles, concepts, practices, processing, and data analysis that are compatible with the study design (Roth, 2006). In this study, this method is used to gather all the information or information from the writings of classical and contemporary scholars related to the concept of cybercrime to build an appropriate theoretical foundation related to the idea based on the current reality in Malaysia. This approach is also applied in identifying the position of cybercrime from Islamic Law perspective. The data is then analyzed inductively through detailed observations in general situations and then moves towards formulating more specific views and theories (Neuman, 2006). Finally, this approach is used to describe the problem or phenomenon that is being studied. Then the findings of the study will be used for the formation of a theory or model that is appropriate to the problem being studied.

Cybercrime in Malaysia

Cybercrime is a form of crime in the modern era that is becoming more prevalent. The misuse of expertise and skills in the internet field has led to the existence of a group of people who tend to commit this crime. It is due to the modus operandi of cybercrime which is felt to be easier and faster without having to put in the effort to involve physical elements in the transfer and misappropriation of property. Cybercrime is criminal behavior that uses any electronic device through an internet service connection. It allows criminal conduct to be committed, whether it involves an individual or a group of people, and can reach the boundaries of one country to another in a short time and unlimited (Anita & Nazura, 2004). Cybercrime can also cause loss or damage to equipment, data, and information involving software or computer processing, whether a virus attack, intrusion (unauthorized access and use) or theft of information against a targeted computer or electronic device (Rusli et. et al., 2003).

The cybercrime that occurs nowadays has brought various negative impacts, including the loss of ringgit money, threats to life and safety, and humiliating the dignity and reputation

of an individual or an organization. It can also threaten a country because of its wider field compared to conventional crime (Mursilalaili, 2003). Cybercrime involves using electronic devices as a medium to commit crimes such as fraud, theft, extortion, forgery, and embezzlement, usually involving the use of the internet (Paul, 2007). In general, there are five primary forms of property cybercrime based on reports submitted to the authorities: hacking, scamming, phishing, forgery of credit cards and bank account cards, and money transfers forbidden.

a) Hacking

The crime of hacking is one of the crimes that often occur in the cyber world today. This crime can disable various central and critical systems involving electronic information databases and security system controls in a country and is seen as a significant threat taken very seriously at the international level. An act can be hacking when cyber criminals try to illegally access a system or break into existing security access (Rahul, 2016). If there are no security restrictions on a website, the intrusion, then the hacking activity is not considered to have taken place. This hacking is usually done to steal data or obtain confidential information without the knowledge or permission of the owner of the computer system (Jain, 2005).

b) Scamming

Cyber fraud is the most straightforward crime to commit because this type of crime does not require high computer skills, whether it involves programming, breaking into, or breaking into the security system of a computer or electronic device. On the other hand, this crime of cyber fraud can be done only by having basic skills with computers or electronic devices and the internet, in addition to a very slick style of fraud in trapping and deceiving victims with uploaded advertisements. In 2016 alone, 3,921 online fraud cases were recorded, and among those crimes were crimes involving fraud schemes and the purchase of goods online and recording an increase of about 20.4% compared to the previous year (Suhael, 2017). Among the sites or pages often targeted by cyber fraud are social media sites such as Facebook, Lazada, Zalora, and Instagram or online business advertisement sites such as Lelong.my, Mudah.my, and various other online mediums for selling goods (Connie, 2015). The value of losses suffered by the victims of this scam also involves tens of ringgit and has reached millions of ringgit. Therefore, it should no longer be taken for granted and is a significant security threat. This act of cyber fraud is straightforward and occurs in many ways and forms. For example, it may happen in buying and selling or business or services offered.

c) Pishing

Phishing is a criminal attempt that involves deception to obtain sensitive information in online electronic communications, such as usernames, passwords, and credit card details, by impersonating a trustworthy entity to obtain data for criminal activity (MAMPU, 2010). Phishing is usually done through applications such as email, short message systems (SMS), or social media sites. In addition, phishing cybercriminals use various forms and methods such as persuasion, blackmail, seduction, and others. The ultimate goal for criminals is to obtain something in the form of financial benefits or property.

d) Forgery of Credit Cards and Bank Account

Forgery of credit cards and bank account cards is one of the most common cyber crimes. Most of the reports received by banks and financial institutions today are where most users report

their money is missing. Even if they do not withdraw the funds on the date stated in their monthly account statement when they check it. Several modus operandi used by credit card counterfeiting syndicates exist in Malaysia. Among the modus operandi used by credit card counterfeiting cybercriminals in Malaysia are (i) Theft of credit card account details, (ii) Use of scanners, (iii) Installing chips on electronic data detection terminals, (iv) Bypassing telephone lines, (v) Collusion, (vi) Phishing email, (vii) False impressions over the phone and (viii) Card forgery through extrapolation and cloning methods (Zain, 2011).

e) Illegal Money Transfer

Illegal money transfer involves transferring money from an individual's or an organization's savings account into another party's bank account or the individual who does the action (Ashriq & Khairunnisa, 2012). This act can also be termed "cyber theft" because it uses the cyber medium as an intermediary in stealing money (Anita & Nazura, 2004). Illegal money transfer means the transfer of funds by a person who does not have permission or authority to access an account owned by an individual or individual and transfer a sum of money into his account or another account and intend to hold the funds. The crime of illegal money transfer through an electronic medium that occurs in Malaysia can be seen as done by individuals with access to transfer money. It happens when the individual abuses power and commits treachery by illegally transferring the money. This crime is classified as a cyber crime because it uses computers or any electronic equipment and systems to commit a crime. There is no act of hacking or breaking in that can be linked to this type of cybercrime because, indeed, this criminal has access and information to enter the system utilizing empowerment and fraud.

Cybercrime from an Islamic Law Perspective

Based on the modus operandi of some property cybercrimes mentioned, it was found that they all involve the same technical aspect, which is the taking or transferring of property or valuable information without the owner's knowledge to steal. This invites questions regarding the position of the property storage element, especially in the new digital format. This debate is necessary considering that the strength of the place where the property is stored is one of the main aspects seen to convict a behavior as a theft crime, according to Islam. Doubts about the quality of this digital property storage will undoubtedly cause defects in the prosecution and conviction of the offense, so it has the potential to result in the perpetrator's belief. In general, four essential elements need to be evaluated in determining the position of the place where the property is stored in today's cybercrime, namely:

a) Concept of Digital Property

In discussing the property and digital storage issue, the jurists, agreed to leave the assessment to the local authority based on the time difference, atmosphere, and domestic location (Fida' Fathi, t.th). Although previous scholars have never discussed the issue of cyber property, it does not mean that this issue does not have a basis for legal evaluation based on Shariah. This means that every property valuable to humans has the right to protection regardless of the medium on which the property is located. The method of jurisprudence states: "Each principle of syar'a for which there is no specific text, but it is parallel to the actions required by syar'a, and its meaning can also be obtained from the dalil of syar'a. So the basis is valid and can be used as a reference. This is because a foundation is formed with solid arguments" (Syatibi, 2003). According to the jurists, every property that can be legally bought and sold is

considered valuable (Nazura & Jasri, 2003). In today's era, property or data stored virtually (*ma'nawi*) has commercial value in society and is very valuable. Therefore, trespassing on this form of property is prohibited by Shariah and entitles the perpetrator to be punished with a determinate sentence.

b) Property Transfer and Acquisition

The process of sentencing for the limit of theft can continue with the removal and transfer of property from the property owner's control to the thief's control. However, if damage occurs during the transfer process, or if the property owner succeeds in getting the property back, then the penalty sentence will be dropped and instead will be transferred to the punishment of takzir. In addition, the element of loss that occurs to the property owner as a result of the loss of the property also qualifies the perpetrator of the crime to be convicted. In the case of cybercrime, although the original physical location of the property is not damaged, only the internal data is transferred virtually. Still, the purpose of sharing the property to possess it without the permission of the owner of the original property is a form of crime despite using a digital medium. This is according to the method: "Medium follows the law of purpose" (Qarafi, 1998). Therefore, in this issue of cybercrime, any invasion of property without rights is prohibited by Shariah. Therefore, any mediation that can lead to the charge is also prohibited and can lead to the implementation of criminal punishment, either hudud or takzir, if successfully convicted by the prosecution.

c) Security Control System Intrusion

An essential element in the conviction of the theft crime is that the property is taken secretly without the property owner's consent. This invasion element must be ensured that it is done with malicious intent by the perpetrator. The two main conditions in ensuring that this criminal conviction can be carried out are first, where the property is stored, is equipped with security features, and meets the minimum security control standards set by the competent authorities. This is because trespassing on property that is not carefully controlled will raise doubts about the control of the property, so the perpetrator may only be tried under the law of impunity (Nazura & Jasri, 2003). Secondly, the thief needs to be sure he has no access to the place where the property is stored, either directly or indirectly. This is because a thief who has any access to the storage place of property belongs to the treason and breach of trust category and is not a theft crime. The crime of treason and breach of trust is not punishable by a determinate sentence as the Prophet SAW said: "The hands of traitors, usurpers and pickpockets are not cut off" (HR al-Tirmidhi).

d) No Element of Reasonable Doubt

Various strict procedures must be followed in convicting a crime with a determinate sentence. The burden of proof for an offense rests on the prosecution. Therefore they have to prove that the accused party is guilty. However, there is a difference in the level of proof between hudud crimes and takzir. For the crime of takzir, the level of evidence is lighter where it is only required that the elements of proof reach the level of zann al-ghalib or in the legal language beyond reasonable doubt (Hamid & Maimoonah, 1993). However, for hudud crimes, the level of proof required to convict an offense is heavier, i.e., the prosecutor must prove the person's offense to the level of al-yaqin or refer to as beyond any shadow of a doubt (Aziz, 1955). Umar al-Khattab said: "Indeed, I do not carry out hudud punishment because there is doubt. It is better than I carry it out with doubt" (Sadiq, 1987).

The level of proof for hudud crimes is considered more challenging because it is mandatory. Therefore, the method of conviction is set to be stricter to avoid any mistreatment and mistakes during the execution of the sentence. Islam does not only emphasize the aspect of retribution but also takes into account the aspect of education for criminals to improve the morals of each individual. In addition, this also aims to ensure that every individual involved gets a proper defense from the judicial institution fairly and equitably, whether on the part of the victim or the criminal. Looking at the threat brought by the advancement of technology and information affecting the whole world, various countries have enacted acts and cyber laws for their respective countries. It is to ensure the existence of control and protection for cyber users from continuing to become victims of cyber criminals who provide various forms of security threats through cyber mediums.

Malaysia is also no exception in enacting acts related to cyber since the beginning of the development of technology and information in this country. This is to ensure that the rule of law and harmony among the community can be established and that cybercriminals are not exempt from any legal action for the actions of those who misuse the cyber facilities provided. Among the cyber law provisions in Malaysia are (i) Computer Crime Act (1997), (ii) Digital Signature Act (1997), (iii) Communications and Multimedia Act (1998), and (iv) Protection Regulations Consumers (Electronic Commerce Transactions) 2012. This law was enacted following the development of technology and communication following the current cybercrime trend. Every year, the development of technology and communication is increasing with various new online services. This invites the abuse of the cyber medium by irresponsible parties. Therefore, the act and regulations become a reference for cybercrime cases that occur in Malaysia, where it is usually read together with other criminal laws in court in convicting for an offense committed.

The advancement of technology and information that has hit the world and society today has brought many conveniences and benefits to the community, especially cyber users. But, inevitably, every progress and facility enjoyed will not escape abuse by some irresponsible parties. Property cybercrime can no longer be taken for granted because the implications of the loss brought by property cybercrime are enormous. Property cybercrimes are generally no different from ordinary theft crimes as they lead to the loss and loss of property due to it being taken or removed without permission from a place of storage. The various forms of cybercrime that often change or increase with time and progress are a challenge to cyber users and law enforcement agencies.

Laws enacted must always follow the current and latest developments in crime to prevent cybercriminals from being subject to any action for criminal conduct. The awareness of cyber users in using all forms of electronic equipment or cyber medium also plays an essential role in reducing the occurrence of cybercrime. This property cybercrime takes advantage of the carelessness and recklessness of cyber users to commit crimes. This is because cyber users are often insensitive to the security aspect of their property storage in cyber form. It is not impossible that in the future, there will be an increase in cases of property cybercrime in addition to the emergence of new forms of property cybercrime because technology and information are constantly developing rapidly and are always changing.

Conclusion

Islam has provided a reasonably systematic and comprehensive way of life that involves the relationship between creatures and the creator and the way of life among human beings. The setting of convictions and punishments for criminal acts is intended to protect the rights and

interests of every human being from being infringed upon and should not be judged as a mere form of tyranny. This is because the main objective of setting punishments in Islam is to provide awareness and teaching rather than just retribution for actions. In the case of sentencing for the crime of theft, the main objective of executing the sentence is to preserve the property rights of fellow human beings. However, the conviction is not carried out quickly. Instead, it is necessary to go through a strict procedure of proof and prosecution to ensure that no party can be wronged through the conviction. In addition, the acceptance of some current methods, such as the involvement of experts, also proves that Islam is a flexible and realistic religion with changing times and atmosphere, especially involving human relationships.

Acknowledgments

This paper is one of the research output made for fulfilling the Incentive Research Grant (Kolej Universiti Islam Melaka) requirement under the project entitled, 'The Influence of ICT Accessibility on Cyber Bullying: A Study Among Melaka Youth' numbered GPI/21/F1/18

References

aAwwa, M. S. (1983). *Fi Usul al-Nizam al-Jina'i al-Islam*. Qahirah: Dar al-Ma´arif.

Amir, A. A. (1985). *al-Ta´zir fi al-Syariah al-Islamiyyah*. Mesir: Dar al-Kitab al-´Arabi.

Anita, A. R., & Nazura, A. M. (2003). "Theft of Information: Possible Solutions Under Malaysian Law", *Malaysia Law Journal* 3.

Anita, A. R., & Nazura, A. M. (2004). *Jenayah Berkaitan Dengan Komputer Perspektif Undang-Undang Malaysia*. Kuala Lumpur: Dewan Bahasa dan Pustaka.

Ansari, Z. M. (2015). *Asna al-Matalib fi Syarh Raudah al-Talib*. Qahirah: al-Matba'ah al-Maymaniyyah.

Ashriq, F. A., & Khairunnisa, S. (2012). "Ancaman Jenayah Siber", laman sesawang *Utusan Online*, dikemaskini 16 April 2012, http://utusan.com.my/info.asp?y=2012&dt=0416&pub=Utusan_Malaysia&sec=Sains_%26_Teknologi&pg=st_01.htm

Asiah, B., Shariffah, N. A. S., & Mohamad, A. M. (2015). Intipan Siber: Jenayah Baru Dalam Masyarakat Kontemporari, *Jurnal Islam dan Masyarakat Kontemporari*, 11.

Astrusyani, M. M. (t.th). *al-Fusul*. Mesir: al-Maktabah al-Markaziyyah bi Masjid al-Sayyidah Zaynab.

Atul, J. (2005). *Cyber Crime : Issues and Threats*. Delhi : Isha Books.

Awdah, A. Q. (t.th). al-Tasyri´ al-Jina'i al-Islam Muqaranan bi al-Qanun al-Waḍ'i. Beirut: Dar al-Katib al-Arabi.

Burnu, M. S. A. (2002). *Mawsu'ah al-Qawa'id al-Fiqhiyyah*. Riyad: Maktabah al-Tawbah.

Fida', F. S. (t.th). *al-Tatbiqat al-Mu´asarah li Syart al-Hirz fi al-Sariqah*. t.tp: t.p.

Gita, R. (2008). *Internet Banking In Malaysia (Part 2) : The Incidence of Fraud and its Prosecution*. Kuala Lumpur:The Law Review.

Hamid, I., & Maimoonah, H. (1993). *Law of Evidence*. Kuala Lumpur: Central Law Book Corporation.

Helmi, M. S. (2015). "Sindiket Pemalsuan Kad Kredit/ATM Tumpas", laman sesawang *Polis DiRaja Malaysia*, dicapai 15 Julai 2015, https://www.rmp.gov.my/news-detail/2014/06/12/sindiket-pemalsuan-kad-kredit-atm-tumpas

Hisyamuddin, A. (2015). "Sindiket Curi Data Palsukan Kad Kredit", laman sesawang *Utusan Online*, dikemaskini 3 Februari 2015,

http://www.utusan.com.my/berita/jenayah/sindiket-curi-data-8232-palsukan-kad-kredit-1.55439

Hummam, K. D. (2003). *Syarh Fath al-Qadir 'ala al-Hidayah Syarh Bidayah al-Mubtadi*. Beirut: Dar al-Kutub al-'Ilmiyyah.

Kasani, A. A. M. (2003). *Bada'i´ al-Sana'i´ fi Tartib al-Syara'i´*. Beirut: Dār al-Kutub al-´Ilmiyyah.

Khayyat, A. A. (1999). *al-Nizam al-Siyasi fi al-Islam*. Qahirah: Dar al-Salam.

Maskun. (2014). *Kejahatan Siber: Suatu Pengantar*. Jakarta: Kencana.

Mawardi, A. M. H. (1994). *al-Hawi al-Kabir fi Fiqh al-Imam al-Syafi'i*. Beirut: Dar al-Kutub al-'Ilmiyyah.

Mohamed, D. (2012). "Investigating Cybercrimes Under the Malaysian Cyberlaws and the Criminal Procedure Code: Issues and Challenges. *Malaysian Law Journal*, 6.

Munir, A. B. (1999). *Cyber Law Policies and Challenges*. Kuala Lumpur: Butterworths Asia.

Mursilalaili, M. S. (2006). *Jenayah Siber Menurut Perspektif Islam*. (Tesis, Fakulti Pengajian Islam UKM).

Mustapa, L., & Sairul, Z. M. (2016). "Godam Pakai Perisian Pasaran Gelap", laman sesawang *Kosmo*, dicapai 17 Disember 2016, http://www.kosmo.com.my/kosmo/content.asp?y=2017&dt=0210&pub=Kosmo&sec=Negara&pg=ne_01.htm#ixzz4kBzYRKWz

Nazura, A. M., & Jasri, J. (2003), "Jenayah Komputer : Perbandingan Menurut Akta Jenayah Komputer 1997 dan Prinsip Undang-Undang Jenayah Islam, *Jurnal Undang-undang dan Masyarakat*, 7.

Nazura, A. M., Anita, A. R., & Hossein, T. (2015), "Cyberspace Identity Theft: An Overview" *Mediterranean Journal of Social Sciences* 6/4.

Norhawa, M. A. (2015). "6,800 Kes Jenayah Siber Di Malaysia Boleh Mengancam Ekonomi Negara", laman sesawang *Utusan Online*, dikemaskini 8 September 2015, http://www.utusan.com.my/berita/jenayah/6-800-kes-jenayah-siber-di-malaysia-1.132952#ixzz4kEw3Wcur

Nuraizah, A. H. (2017). "Undang-Undang Siber: Akta Tandatangan Digital 1997 dan Akta Jenayah Komputer 1997". (Makalah, Simposium Kebangsaan Kerajaan Elektronik, Kuala Lumpur, 18-19 Disember 2017).

Qarafi, A. I. (1998). *Anwar al-Buruq fi Anwa´ al-Furuq*. Beirut: Dar al-Kutub al-´Ilmiyyah.

Qudamah, A. M. (1997). *al-Mughni*. Riyad: Dar ´Alim al-Kutub.

Sadiq, M. (1987). *al-´Uqubat al-Syar´iyyah wa Mauqifuhāa fi al-Nizam al-Ijtima´i al-Islami*. Qahirah: al-Zahra' li al-I´lam al-´Arabi.

Sadlan, S. G. (1986) *al-Qawa´id al-Fiqhiyyah al-Kubra*. Riyad: Dar al-Balansiyah.

Sahizan, S. (2015). *Awas! Jenayah Siber*. Kuala Lumpur: Dewan Bahasa dan Pustaka.

Shabl, A. A. I. (2012). *al-I'tida' al-Ilikturuni*. Riyad: Dar Kunuz Isybiliya.

Shamsuddin, S. (2016). *Jenayah dan Kanun Keseksaan*. Kuala Lumpur: Dewan Bahasa Dan Pustaka.

Sharbini, M. K. (1997). *Mughni al-Muhtaj ila Ma´rifah Ma´ani Alfaz al-Minhaj*. Beirut: Dār Ma´rifah.

Shatibi, I. M. M. (2003). *al-Muwafaqat* (Qahirah: Dar Ibn ´Affan.

Syawkani, M. A. M. (2005). *Nayl al-Awtar min Asrar Muntaqa al-Akhbar*. Riyad: Dar Ibn Qayyim.

Tamrin, A., & Ainnur, H. A. M. (2015), "Undang-Undang Siber Dari Perspektif Islam", *Jurnal Teknologi* 72/1.

Zaki, M. (2008). "Jenayah Komputer dan Jenayah Siber: Menangani Ancaman" dalam *Transformasi Masyarakat: Cabaran Keluarga, Gender dan Sosiobudaya* ed. Rahman Abdul Aziz. Bangi: Penerbit UKM.

Zuhayli, W. (1985). *al-Fiqh al-Islami wa Adillatuhu*. Damsyik: Dar al-Fikr.

Zuhrah, M. A. (1998). *al-Jarimah wa al-´Uqubah fi al-Fiqh al-Islami*. Kaherah: Dar Fikr al-´Arabi.