THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 13 | Number 3 Article 5

9-30-2018

Sharia Law and Digital Forensics in Saudi Arabia

Fahad Alanazi
De Montfort University

Andrew Jones
University of Hertfordshire

Catherine Menon
University of Hertfordshire

Recommended Citation

Alanazi, Fahad; Jones, Andrew; and Menon, Catherine (2018) "Sharia Law and Digital Forensics in Saudi Arabia," *Journal of Digital Forensics, Security and Law*: Vol. 13 : No. 3 , Article 5.
DOI: https://doi.org/10.15394/jdfsl.2018.1568
Available at: https://commons.erau.edu/jdfsl/vol13/iss3/5

SHARIA LAW AND DIGITAL FORENSICS IN SAUDI ARABIA

Fahad Alanazi
Cyber Security Center
De Montfort University
Fahad3n@hotmail.com

Andrew Jones
Cyber Security Centre,
University of Hertfordshire
Security Research Institute, Edith Cowan University
andy1.jones@btinternet.com

Catherine Menon
School of Computing
University of Hertfordshire
c.menon@herts.ac.uk

ABSTRACT

These days, digital crime is one of the main challenges for law enforcement and the judicial system. Many of the laws which are used to protect the users of current technologies were derived from legislation and laws that are utilized in the control of crimes that are based in the physical realm. This applies not only in Western countries, but in countries that adopt Sharia law. There is a need to establish specific legislation and accepted best practice to deal with digital crimes that is compatible with Sharia law, which affects more than one billion Muslims. This paper presents a view of the approach to digital crime in Saudi Arabia under Sharia Law, demonstrating how this is founded on principles from the Qur'an and the Sunnah, which are the sayings and deeds of the Prophet Muhammad. We describe how Sharia law differs from Western law, and how evidence for digital forensics procedures can be obtained for use under Sharia law.

Keywords: Sharia law; digital forensics, Law, Procedure, Saudi Arabia

1. INTRODUCTION

The digital investigation processes are basically the procedure which allows the outcomes of investigation into incidents of inappropriate behaviours and illegal and criminal activities to be of a quality which can be submitted to a court of law (Carrier, 2006). There are many digital investigation models and frameworks for procedures which have been developed around the world during the past three decades (Brill and Pollitt, 2006). The digital investigation processes should follow a number of steps to achieve a successful outcome to a digital forensics investigation (Carrier, 2006). A number of models or frameworks are used by organisations to enhance their investigation procedures to ensure that evidence for

presentation in the court is of an acceptable standard (Brill and Pollitt, 2006). Thus, since as early as 1984, law enforcement agencies, such as the FBI laboratory, made efforts to enhance the processes of digital investigations (Perumal, 2009). In order to avoid the risk of inadmissibility of the evidence in the court, appropriate investigative processes need to be followed. Based on our observations, there are a number of digital investigation processes and frameworks that have been proposed, some of which tend to be applied to the wider environment and others applied to specific scenarios (Alanazi, Jones, 2017).

Forensic science emerged in response to a need to uncover the facts behind inappropriate, illegal and criminal activities. The role of forensics can be represented using forensics models, techniques and methodologies and by following the commonly accepted stages of an investigation; i.e. evidence preservation, collection, analysis and presentation to the courts. The digital forensics process follows the same stages of investigation as traditional forensics.

This paper looks at the use of digital forensics under Sharia law in Saudi Arabia through the establishment of rules which takes into account social development within the ethical standards that are based on the Qur'an and Sunnah. Also, it discusses the application of digital forensics in Saudi Arabia that have been applied, based on Sharia law, and some of the issues regarding the collection of evidence. In addition, it shows how the use and interpretation of the Qur'an allows many of the digital crimes to be addressed using traditional approaches. It has also highlighted some of the areas where there is potential for the development of either new laws or new procedures within the framework of Sharia to address the issues of the way that digital evidence is perceived and received in the courts.

2. SHARIA LAW

Sharia law arose with the coming of the Prophet Muhammad in the seventh century, which gave rise to the birth of Islam. Sharia law is the common Law within the Islamic religion to guide the Muslim people in their daily lives. Sharia law is described as the way to follow God's (Allah's) Law (Wiechman et al., 1994).

Sharia law is derived from several sources. The first and main source is the Qur'an, which Muslims believe was verbally revealed by God to the prophet Muhammad through the angel Gabriel over a period of around 23 years, beginning in 609 Common Era (CE), when Muhammad was aged 40, and concluding in 632 CE, the year of his death. (Fisher, 1997) The Qur'an addresses all of the important aspects of human life, including the relationship between God and people and between people and society, including ethics, jurisprudence, social relations, justice, politics, law, morality, trade and commerce. (Alfaize, 2015), (Ansary, 2015).

The second source is the Sunnah, which literally meaning a path, method or way, contains those religious practices that were established by the Prophet among his companions and which have been passed on by the consensus of generations. (Farid, 2017)

The Hadith on the other hand, literally means something new, which may be a saying or a statement and refers to narrations that are attributed to the companions of the Prophet, who narrated a statement or a story about the Prophet or related to the Prophet. The Hadith has been passed on through an individual or a few narrators in every generation (Farid, 2017).

If the answer is not found in these sources then Ijma, which refers to the consensus of opinions, is the next source of law. It is a way

of discovering the law by resorting to the general consensus of opinion among Ulema or Sharia scholars of a particular era. The prophet is reported to have stated that that if all Muslims agree on a matter, then it cannot be wrong (Alfaize, 2015).

When the Ulema (scholars) fail to find a resolution from the Qur'an, Sunnah, or Ijma, they may use Qiyas or analogical reasoning from principles established in the Qur'an or Sunnah. For an example of how this may be applied, modern 'recreational' drugs are not explicitly mentioned in the Qur'an or Sunnah. However, alcohol is mentioned, and it is prohibited because of its effects on the body and mind, as it impedes a person's ability to perform their religious obligations. The same harm is at issue in the case of drug-taking as of drinking; thus, the same rule (prohibition) is applied (Alfaize, 2015).

There are three major crime groups under Sharia law: 'Hadd' Crimes are serious crimes such as Murder; robbery; apostasy (the abandonment or renunciation of a religious or political belief or principle) from Islam, making war upon Allah and his messengers (the prophet Muhammad); fornication; theft; defamation; false accusation of adultery and the consumption of intoxicants. The punishment of these crimes is pre-established in the Qur'an and Sharia law does not allow the judge to reduce or change the punishment of these crimes because they were 'set by God' and found in the Qur'an. Sharia law considers the higher level of proof and the reasons which led the person to commit the crime; this can be through confessing to the crime or through sufficient witnesses to the crime. When there is no confession, not enough witnesses or doubt about the guilt; Sharia law will punish these crimes as a 'Tazir' crime (Madkoar, 1980).

'Tazir' Crimes are less serious than 'Hadd' crimes. 'Tazir' crimes are the acts that are considered to cause harm to the societal interest and the punishment of these crimes are not pre-established in the Qur'an as are 'Hadd' crimes. Sharia law seeks to work in the societal interest and prevent such crimes from being committed. 'Tazir' punishments vary according to the seriousness of the crime. In this area, Sharia law is flexible, where the judge, through Sharia law in a 'Tazir' crime, is free to set the punishment based on many factors such as customs and local norms, in order to deter and rehabilitate the offenders. The common punishments for 'Tazir' crimes are: fines, seizure of property, flogging and imprisonment (Madkoar, 1980).

In 'Qisas' Crimes, which are typically revenge crimes, the penalty may include restitution. The punishments for these crimes are set in the Qur'an, where 'Qisas' punishments have many forms including 'Diya', which is the monetary payment of damages to the victim. For example, if somebody is killed; his family has the right to ask for 'Qisas' punishment for the offender or to ask for 'Diya'. Any victim of a crime has the right to seek retribution, as the Qur'an states "And We ordained for them therein a life for a life, an eye for an eye, a nose for a nose, an ear for an ear, a tooth for a tooth, and for wounds is legal retribution." the Qur'an. (Al-Maaida. pp.S.5. A.45) (Madkoar, 1980) (Abbas, 2009).

3. DIGITAL CRIME

The digital world has created new opportunities and methods of committing crime. Crimes related to the digital world continue to grow significantly with the development of technology and this is reflected in the growing concerns over the threat of digital crime. To date, in Saudi Arabia, there has been a lack of understanding of offenders' behaviour and lack of best practice to deal with digital crimes that is compatible with Sharia law in this new environment.

There are experts in a number of fields in law in western nations that have participated in assessments and contributed to the modification of the existing laws in their respective countries to ensure that the laws are suited to, and updated to address digital crimes, for example as early as 1990, the UK government introduced the Computer Misuse Act (UK Govt, Computer Misuse Act, 1990).

4. DIGITAL CRIME IN SAUDI ARABIA

Unlike in the West, where technology is seen as both a new medium for existing crimes such as fraud and theft and also as a platform for new types of crime, such as Denial of Service (Brenner S et al, 2001), from the Islamic point of view, digital crimes have not been thought of as a new type of crime but only a new method of committing existing crimes (Alfaifi, 2001).

One of the problems faced in assessing digital crime is that technology has facilitated crimes that have none of the conventional national and legislative boundaries. As a result, Muslims lean towards following the Islamic teachings in assessing digital crime.

4.1 Saudi Arabian Law

Saudi Arabian law is based on Sharia law. However, Saudi Arabia does take into account the different religious sects and faiths, and there are courts available to accommodate those groups of Muslims that follow their differing beliefs. These courts address religious differences and are for solving the issues that are faced by them, for examples there is a court in al Qatif city for the Shia sect to solve personal issues and everything related to doctrinal beliefs such as fasting issues, social issues or praying issues. In addition, Sharia law in Saudi Arabia guarantees to non-Muslims their human rights, as long as they live under the umbrella of Islamic rule (Al Hwaimel, 2009).

4.2 Privacy and Sharia law

The Islamic approach to protecting privacy, which can be used to include digital devices, is based on the Qur'an. This can be seen in an example where the Qur'an gives the proper etiquette for visiting one another. According to the Qur'an, Allah Said "O you who have believed, do not enter houses other than your own houses until you ascertain welcome and greet their inhabitants. That is best for you; perhaps you will be reminded" the Qur'an. (An-Noor. pp.S.24. A.27) (Islamweb, 2009). Therefore, the Islamic principles ask Muslims to gain permission before they access the properties of another. Based on this principle, a person must not gain access to digital devices (physically or logically) which are not his own or look at their contents without permission.

The Islamic approach to protecting data and privacy etc. is based on the principle that urges individuals not to spy on the secrets of others, which can logically be extended to include those contained in digital devices. This can be seen, for example where, in the Qur'an, Allah said: "O believers! Avoid immoderate suspicion, for in some cases suspicion is a sin, do not spy on one another" (Al-Hujurat, 12) (Malik, 2001).

One fundamental difference between the approach taken in the West and the Islamic approach is that under Sharia law any illegal access to another person's property without permission is considered as theft. This is taken from another quote from the Qur'an, in which Allah said: "The thief, the male and the female, amputate their hands in recompense for what they committed as a deterrent [punishment] from Allah. And Allah is Exalted in Might and Wise." the Qur'an. (Al-Maaida. pp.S.5. A.38).

4.3 Anti-Cyber Crime Law

Legislators in Saudi Arabia have recognised that the traditional procedural rules are not always suitable or applicable to cybercrimes and have therefore introduced new procedural rules better suited to electronic communications (Atalla, 2010).

The Anti-Cyber Crime Law was issued under the Council of Ministers Decision No. 79, dated 7/3/1428 H, and it was approved by Royal Decree No. M/17, dated 8/3/1428H. The Act was published in the Issue No (4144) of the Official Gazette (Um Al Qura) on 13/04/1428H.

In Saudi Arabia, cybercrime and the appropriate punishments are defined in Articles 3 to 9 of Royal Decree M/17 of 2007 - Anti-Cyber Crime Law in Table 1.

Table 1
Anti-Cyber Crime Law Articles

Article 3: Any person who commits one of the following cybercrimes shall be subject to imprisonment for a period not exceeding one year and a fine not exceeding five hundred thousand riyals or to either punishment: 1. Spying on, interception or reception of data transmitted through an information network or a computer without legitimate authorization. 2. Unlawful access to computers with the intention to threaten or blackmail any person to compel him to take or refrain from taking action, be it lawful or unlawful. 3. Unlawful access to a web site or hacking a web site with the intention to change its design, destroy or modify it, or occupy its URL. 4. Invasion of privacy through the misuse of camera-equipped mobile phones and the like. 5. Defamation and infliction of damage upon others through the use of various information technology devices.
Article 4: Any person who commits one of the following cybercrimes shall be subject to imprisonment for a period not exceeding three years and a fine not exceeding two million riyals or to either punishment: 1. Acquisition of movable property or bonds for oneself or others or signing such bonds through fraud or use of false name or identity. 2. Illegally accessing bank or credit data, or data pertaining to ownership of securities with the intention of obtaining data, information, funds or services offered.
Article 5: Any person who commits one of the following cybercrimes shall be subject to imprisonment for a period not exceeding four years and a fine not exceeding three million riyals or to either punishment: 1. Unlawful access to computers with the intention to delete, erase, destroy, leak, damage, alter or redistribute private data. 2. Causing the information network to halt or breakdown, or destroying, deleting, leaking or altering existing or stored programs or data. 3. Obstruction of access to, distortion, and causing the breakdown of services by any means.

Article 6: Any person who commits one of the following cybercrimes shall be subject to imprisonment for a period not exceeding five years and a fine not exceeding three million riyals or to either punishment:

1. Production, preparation, transmission, or storage of material impinging on public order, religious values, public morals, and privacy, through the information network or computers.
2. The construction or publicizing of a web site on the information network or computer to promote or facilitate human trafficking.
3. The preparation, publication, and promotion of material for pornography or gambling sites which violates public morals.
4. The construction or publicizing of a web site on the information network or computer to trade in, distribute, demonstrate method of use or facilitate dealing in narcotic or psychotropic drugs.

Article 7: Any person who commits one of the following cybercrimes shall be subject to imprisonment for a period not exceeding ten years and a fine not exceeding five million riyals or to either punishment:

1. The construction or publicizing of a web site on the information network or computer for terrorist organizations to facilitate communication with leasers or members of such organizations, finance them, promote their ideologies, publicize methods of making incendiary devices or explosives, or any other means used in terrorist activities.
2. Unlawful access to a web site or an information system directly, or through the information network or any computer with the intention of obtaining data jeopardizing the internal or external security of the State or its national economy.

Article 8: The imprisonment and the fine may not be less than half the maximum if the crime is coupled with one of the followings:

1. The crime is perpetrated through organized crime.
2. The offender holds a public office and the crime perpetrated relates to this office, or if he perpetrates the crime using his power or influence.
3. The luring and exploiting of minors and the like.
4. The offender has been previously convicted of crimes within or outside the Kingdom.

Article 9: Any person who incites, assists or collaborates with others to commit any of the crimes stipulated in the Law shall be subject to a punishment not exceeding the maximum punishment designated for such crimes, if the crime is committed as a result of said incitement, assistance or collaboration, and he shall be subject to a punishment not exceeding half the maximum punishment designated, if the intended crime is not committed.

However, according to Elguindy (2012), The Saudi 'Anti-Cybercrime law' and the 'special cybercrime system' cannot be considered a complete cybercrime law as it does not contain specific methods defined for examining such crimes. According to this law, a number of online actions could be interpreted as cybercrime due to absent or unclear definitions.

5. DIGITAL FORENSICS IN SAUDI ARABIA

In Saudi Arabia, there are currently no specific guidelines for the collection, processing and handling of digital evidence and digital forensic investigations. There are policies and principles related to computer incident response that have been set out and adopted within Saudi Arabia (CERT), however, to date, there is no officially recognised procedure for digital forensic investigations. As a result, because of the lack of official guidelines and accepted best practice, these principles have not been considered to have met the prerequisite of Islamic law investigation in Saudi Arabia for there to be an officially acceptable level of proof. According to Stamatel and Sung, (2010), "The standard of proof is high in Saudi Arabia and the courts generally follow the stringent rules of Islamic Law. The rules require a number of witnesses of particular kinds, and the accused is considered innocent until proved otherwise. For some hudud *(the plural of Hadd)* crimes (acts against God), which include apostacy, rebellion, theft, adultery, defamation and drug offenses, the standard of proof is especially high – so high that it is not often adhered to in Islamic courts, except after fulfillment of the conditions of proof" the authors go on to give examples which include "For crimes against persons, witnesses or confessions are also required as proof. Various types of homicide, assault, and fraud usually require two

witnesses. Further, not just any witness is acceptable in the Islamic courts; non-Muslim testimony is not accepted, and witnesses must be male (although in some cases two females can be substituted for one male) and have sound mind and character." When dealing with technology-based crimes this may be very difficult to achieve.

The purpose of a criminal investigation in Sharia law is to find out what actually happened and ensure equity between individuals. This incorporates reporting and derivation. Reporting is to ascertain that the crime has been committed, because the prophet Muhammad (peace upon him) stated that "Were people to be given everything that they claimed, men would [unjustly] claim the wealth and lives of [other] people. But, the onus of proof is upon the claimant, and the taking of an oath is upon him who denies" (Islam Hadiths, Hadiths 32-34, Nawawi). Derivation is defined by Sharia law as information provided as evidence. It is characterised as giving personal private evidence in light of the fact that it is not referred in the Qur'an and the (Hadith) (Dafiri 2003). These days, derivation is known as a methodology for gathering evidence in forensic procedures to verify that a crime has been committed in light of the fact that it is mentioned in the Qur'an that, "If there comes to you a disobedient one with information, investigate, lest you harm a people out of ignorance and become, over what you have done, regretful ..." the Qur'an. (Al-Hujuraat, pp.S.49. A.6). As a result, digital investigators must consider the requirements of Sharia law with regard to evidence, such as admissibility, privacy, integrity and availability of evidence.

The internationally accepted processes and procedures for digital forensic investigations may not meet the requirements of Saudi law, because the legal regulations of each country reflect the reality of trends and tendencies in society. For example, in response to the UK Computer misuse act; when the evidence is compelling, some defence lawyers have been known to try to attack the credibility of the examiner who carried out this act or the processes that were followed. In Saudi Arabia this would be a problem because there is a disparity between the scientific and impersonal nature of western legal systems, which are dependent on scientific evidence, and the ethic and religious commitment of the Islamic religion, which is dependent on faith and trust.

The ways of demonstrating proof in an Islamic court are not limited. Hence, the accepted methods, procedures and practices that they must adhere to, in order to guarantee avoiding disbelief and denial in Islamic court are: witnesses, confession, oath, documents and also arguments, presumptions and preview by the judges of the testimony of experts who help to provide the required knowledge of sciences, such as the testimony of a doctor and the scientific experts (Studies and Research Department, 2013).

In Saudi Arabia the judges do not yet trust the expertise or the best practices of digital forensic practitioners that are recognized in the west and therefore do not trust the digital evidence they produce (Alfaize 2015). Therefore, the judges will most probably use their trust in human witnesses (including digital forensics experts), instead of scientific processes to ensure the authenticity of digital evidence. This is due to prevailing traditionalist views which distinguish Saudi Arabia culture. In comparison, in western countries emphasis is placed on the trustworthiness of the process for obtaining digital evidence (rather that human - i.e. experts). This means if there any doubt about the evidence authenticity, the process itself can be visible, tractable to be investigated and checked. (Alfaize, 2015).

In Saudi Arabia, a judge's acceptance of digital evidence depends in part on the judge's level of use and understanding of digital equipment. As a result, judges do not always make decisions that are consistent with the strength of the laws related to digital evidence. However, digital evidence could be accepted in the court as Confession (Iqrar) but not as Bayyinah (Clear or strong evidence). Furthermore, it is not a matter of if it is considered equal, lower, or higher than other definitive evidence, but is a matter of how this digital evidence has been collected and how it ties in with the crime scenario. Digital evidence might not be accepted at all, or it may be accepted as very low or very strong evidence but will not be accepted as Bayyinah. Digital evidence is still not thought to be good enough to be considered as a clear evidence, in the same way that DNA is still not considered to be very strong, although it is more advanced than digital evidence.

The Saudi courts still have difficulty with digital evidence for discovering proven evidence; this is largely because there are no visible signs. There is no clear evidence of violence or blood, just data and figures, which can be changed or erased from the records, stored in the memory of digital devices, and may not have an external physical impact because the digital crime was targeting intangible property. Therefore, the investigator must be conscious of the Sharia law principles during the investigation in order to ensure that the evidence is admissible in an Islamic court.

6. OBTAINING EVIDENCE OF DIGITAL CRIME IN SAUDI ARABIA

In Sharia law, it is necessary to obtain evidence when the victim reports the crime. Ways of demonstrating a crime in Sharia law have been open to dispute (Alkarmi 2005; Al-Zohaili 1994). There are two perspectives: The primary perspective accepts that such strategies are restricted to particular routines, for example, witnesses, confessions and oaths. This perspective is focused around the Qur'an and the Sunnah (everything that was attributed to the Prophet Muhammed, including sayings or deeds or reports and after him, his companions, and then Affiliates and so on) (al-Munajjid, 2016). This is the traditional view and is based on the Qur'an, from the commandment of the Prophet Muhammad, who is quoted to have said: "I left among you two things, you will never go astray after them: the Book of Allah, and my Sunnah" (Wathakker.info, 2012). (Al-Zohaili 1994).

The second perspective accepts that the techniques that can be used are boundless and can incorporate any system that explains reality, for example, confessions, evidence that is available against the offenders, witnesses, bearing affirmation (the act of confirming something to be true, or is a written or oral statement that confirms something is true) (Al Qarinah) and the product of the investigative techniques used.

Many investigators and lawyers believe that the courts currently still give a low weighting to digital evidence, but it is not clear if it is because of the difficulties in presenting digital evidence in a court or that the members of the court do not understand the concept of digital evidence. This problem is exacerbated by the issues of a lack of personnel with the required skills and a lack of defined procedures and best practice for the search, collection, seizure, and analysis of digital evidence and as a result there is no accepted best practice. If the digital evidence is not collected in a prescribed manner, then the digital evidence that is collected could be of questionable

evidential value. Currently, a lot of digital evidence is excluded because the seizure was conducted by non-technical people before being forwarded to experts for analysis. As a result, the chain of custody and use of tested procedures could not be proven.

Article 124 of the Law of Procedure before Shariah Courts allows the court, when required, to appoint one or more experts. It will define the job of the expert, the time for placing his report and the time for the trial hearing based on the record. However, article 134 clearly states that the experts' opinion is not binding on the court, which merely uses it as a guide. What this does, in effect, is to create a situation where, because of the knowledge required for the collection and processing of digital evidence, the person undertaking the work will be considered to be an expert and as a result the findings are considered as a guide, rather than fact.

However, as technologies and knowledge develop, the general rules on the ways in which proof is provided means that there is the opportunity to plug loopholes in the regulations. In general, Sharia law shows caution with regard to the freedom of the judge in tracking legitimate non-Islamic methods in order to avoid confusion, manipulation, fraud, loss of the judiciary time, and ongoing arguments between the parties.

In the Islamic legal system, the process of digital forensics comprises looking for evidence, gathering evidence, preserving evidence and presenting the digital evidence from a computer, and all of phases of an investigation are compatible with those used in the West. However, in the case of an investigation involving networks, this means that there is a potential conflict between the specialised procedures used in the West to gather digital evidence and the forensics procedure principles in Saudi Arabia. The criminal justice system faces challenges that need to be overcome. Some instances of those challenges are: digital crimes targeting intangible property, the evaluation and adoption of the legality for data which is provided by digital evidence laboratories, the diversity and multiplicity of digital devices and the lack of a stable law or rules for digital evidence (Al Beshri, 2008). Hence, the investigator must be conscious of the Sharia law requirements during the investigation in order to ensure that the evidence is admissible in an Islamic court. There is currently no specialized technical investigative standard for dealing with digital evidence under Sharia law (Al-Murjan and Xynos, 2008).

Because there is a need to protect electronic transactions and to recognise the importance of regulating electronic transactions to avoid digital crimes, the Council of Ministers in Saudi Arabia approved a regulation regarding the Electronic Transactions Protection Law (promulgated by Royal Decree No. M/8 of 26 March 2007), with the aim of reducing digital crimes. The regulation included details on the identification of the target system, the estimation of penalties for each crime and infraction and determining the jurisdiction and application of the sanctions (Atalla, 2010). Article 24 of the regulation states that “Without prejudice to any severer penalty provided for in any other law, anyone found guilty of any of the actions set forth in Article (23) of this Law shall be subject to a fine not exceeding five million riyals, imprisonment for a period not exceeding five years or both penalties. Equipment, systems and programs used in committing the violation may be confiscated pursuant to a judgment.”

The Saudi regulation defines the computer in the first article of the regulation regarding electronic transactions as any digital device, fixed or movable or wired or wireless, that contains systems for data processing, storage,

sending, receiving or browsing and carrying out functions determined according to the programmes and commands that is given (ref. Article 1.7 of the Electronic Transaction Regulation and Article 1.6 of the Cybercrime Regulation) (Atalla, 2010).

In addition, the Saudi regulations on electronic transactions defines electronic transactions as any exchange or correspondence or contact or other procedure concluded or implemented by electronic methods (Article 1.10). Electronic data is defined as data that has a number of characteristics including text, symbols, images, sounds, drawings or other electronic data (Article 1.11) (Atalla, 2010). Before the issuance of this regulation, the substantive rules were guided by traditional texts in Islamic law and the penal regulation of the criminalisation of theft, fraud, breach of trust and forgery were used for protecting data by the law (Atalla, 2010).

Evidence in Sharia law is interpreted as being a sign, which could help find the answer to a riddle. There are various rules for gathering data as evidence in Sharia law as shown below (Al-Zohaili, 1994):

- The evidence must be the result of an investigation: the evidence ought not to be speculated or anticipated, the evidence ought to be extracted by scientific methodology;
- The evidence must connect a crime with its victim or crime and its culprit. In the event that there is a solid connection between them this evidence is called strong evidence, otherwise it is powerless evidence. Strong evidence is adequate in Sharia law as a primary strategy for evidence; powerless evidence is inadmissible in light of the fact that it is considered to be based on prediction.

Therefore, from the outset, the specialist investigator must keep these principles and rules in mind when gathering and collecting data about the crime, for example when listening to witnesses and meeting the victim (Dafiri, 2003).

Nowadays, computer abuses/crimes necessitate that exceptional processes be used to identify the guilty party. Seeking, gathering and examining data helps to find the evidence to accomplish this.

7. DIGITAL FORENSICS PROCEDURE IN SAUDI ARABIA

Forensic procedures to be followed for gathering data as evidence and exploring and securing a decision to punish the guilty in Sharia law were drawn up by the Saudi Arabian Government (Dafiri 2003). However, these procedures address the wider issues of forensics and are not directly relevant or applicable to digital forensics. This is similar to the situation in the west, where ISO 17025 (General requirements for the competence of testing and calibration laboratories) has been adopted. When a crime occurs in a Muslim society, evidence is required to back the claims on the grounds that the Qur'an states "Produce your proof, if you should be truthful" the Qur'an. (An-Naml, pp.S.27. A.64).

An investigation in Saudi Arabia is described as demonstrating a crime with acceptable evidence (Dafiri 2003). A forensic investigation is a set of procedures and lawful strategies that are followed by investigators before a trial to find out the facts and identify the guilty party by assessing and investigating the evidence of crime (Dafiri, 2003). Various forensic investigation procedures could be used, for example, searching for specific evidence of a crime against private property (Dafiri, 2003). It is a technical process to discover a

connection between a crime and a suspect, keeping in mind the end goal, which is to demonstrate whether there has or has not been a crime. This strategy incorporates the following steps:

1. The first step of the search in an investigation is to seize the evidence for a particular crime. Seizing is defined as holding evidence with lawful power, keeping in mind the end goal is to secure the integrity and accessibility to any evidence (Dafiri, 2003). Seizing is done to demonstrate a claim as well as to disprove a claim.
2. The second step is the inspection phase, which seeks to provide the entire picture of the crime by demonstrating the connection between a crime scene and a suspect or between a suspect and a victim. This stage is imperative in light of the fact that it will demonstrate or negate the connection between a suspect, a crime and the seized items.
3. The third phase involves engaging an expert; someone with a high level of expertise in digital forensic investigative procedures and using their skills to connect a suspect with a crime scene. In Islam it is permitted to have an expert witness (Dafiri, 2003) as stated in the Qur'an, "So ask the people of the message if you do not know" " the Qur'an. (An-Nahl, pp.S.16. A.43).
4. The final step is providing answers to questions regarding what kind of crime that was committed, the type of evidence gathered, how it was gathered, what happened, when and by whom (Al-Murjan and Xynos, 2008).

8. CONCLUSION

This paper has presented the investigation of digital crimes from an Islamic view, in the context of Saudi Arabia; with evidence from the Qur'an, Hadith and Sunnah that has shown the principles which are followed by Muslims. It has also outlined the application of digital forensics in Saudi Arabia that have been applied based on Sharia law and highlighted some of the issues regarding the collection of evidence. It has shown that the use and interpretation of the Qur'an allows many of the digital crimes to be addressed using traditional approaches. It has also highlighted some of the areas where there is potential for the development of either new laws or new procedures within the framework of Sharia to address the issues of the way that digital evidence is perceived and received in the courts.

As there is a disparity between the scientific and impersonal nature of western legal systems, and the ethic and religious commitment of the Islamic religion, which is dependent on faith and trust, further research is required into the concepts of trust, reliability and authenticity in order to address the individual dimensions in further detail in Saudi Arabia, and also in other countries and societies (some with less respect for tradition than Saudi Arabia) (Alfaize, 2015) and to identify what are the necessary and desirable characteristics of evidence under Sharia law.

In future work we will also consider the extension of this investigation to include autonomous systems in the domains of justice and law. Such systems model legal reasoning using artificial intelligence techniques to identify theories (Bench-Capon and Sartor, 2001). The conclusions formed may be used to provide sentencing advice, or to support interpretation of legal precedents. Such advisory systems can create uncertainty around where the responsibility lies for actions taken based on these conclusions, and their applicability under Sharia law is not fully determined. Autonomous systems are also

vulnerable to misuse and cyber-crime, particularly where there is no human intervention and therefore no human oversight. The implications of cyber-crime affecting autonomous systems in the domain of Sharia law and justice is still an open question.

REFERENCES

Abbas, N. H. (2009). Qur'an'search for a concept' tool and website (Doctoral dissertation, University of Leeds (School of Computing)), Retrieved from https://pdfs.semanticscholar.org/7064/5274d24fb057ea499233fd66a57cd19dcf6c.pdf.

Abdel-Baky, M.F. (1951). Al-Mowatae of Imam El-Aema wa Alem El Madina, Malek Ibn Anas, El-Shaeb Book. Husn El Kholok, Hadith # 8, p. 564.

Alanazi, F. M. and Jonse (2017). A Method to Enhance the Accuracy of Digital Forensics in the Absence of Complete Evidence in Saudi Arabia

Al Beshri Mohammed. (2008). Habilitation investigators for computer crimes and Internet networks. Naif Arab University for Security Science. 1 (1), 33-34

Alfaifi, M.A. (2001). The Economic Crimes Adjudgments in the Computer. Al-Hakeem, Mohammad Bin Abdullah (1990). Almustadrak, Dar Alkutob Publish, 1990. (In Arabic).

Alfaize, NA. (2015). The Impact of Culture and Religion on Digital Forensics: The Study of the Role of Digital Evidence in the Legal Process in Saudi Arabia.

Al-Hakeem, Mohammad Bin Abdullah (1990). Almustadrak, Dar Alkutob Publish, 1990. (In Arabic).

Al Hwaimel, A. (2009). The application of the Sharia and its impact on the Nations. Riyadh: Dar Ibn Al Atheer. 1-48.

AlKarmi, A. (2005), The Wisdom Methods of Al Sharia Politics, Bit Alafkar, Libnon.

Al-Murjan, A., & Xynos, K. (2008, April). Network Forensic Investigation of Internal Misuse/Crime in Saudi Arabia: A Hacking Case. In Proceedings of the Conference on Digital Forensics, Security and Law (pp. 15-32).

Al-Zuhaili, W. (1994). Fiqh & Perundangan Islam. Dewan Bahasa dan Pustaka, Kementerian Pendidikan.

Ansary, A. (2015). A Brief Overview of the Saudi Arabian Legal System. New York: Hauser Global Law School Program, New York University School of Law.

Ariane. (2013). How to forgive those who have hurt you, even when it's difficult. Retrieved from http://decodingeden.com/how-to-forgive-others-fault-even-when-its-difficult/.

Atalla, S. (2010). The fight against cybercrime in Saudi Arabia. Retrieved from King Saud University: http://faculty.ksu.edu.sa/shaimaaatalla/Pages/crifor.aspx.

Avison, D., Dwivedi, Y.K., Fitzgerald, G. and Powell, P., (2008) The beginnings of a new Era: Time to reflect on 17 years of the ISJ, Information Systems Journal, Vol. [18], No. 1, pp.5-21.

BCS. (2006), Presenting digital evidence to court. Retrieved from http://www.bcs.org/content/ConWebDoc/7372.

Bench-Capon, T. and Sartor, G., (2001) A model of legal reasoning with cases incorporating theories and values, Artificial Intelligence Journal, Vol. [150], Issue 1 – 2, pp.97-143.

Binothaimeen (2007), Library reading: Talk: Explain Session: Talk Third Session, Retrieved from

http://www.ibnothaimeen.com/index.shtml .

Biomedical research ethics: An Islamic view, part I. International Journal of Surgery, (2006). Retrieved from https://www.sciencedirect.com/science/article/pii/S1743919106000975

Brenner S et al, (2001), Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law, Murdoch University Electronic Journal of Law, Volume 8, Number 2

Brill AE, Pollitt M. (2006). The evolution of computer forensic best practices: an update on programs and publications. Journal of Digital Forensic Practice, 1:3–11.

CERT, Saudi Arabia, Make an Incident Response Plan, http://www.cert.gov.sa/index.php?option=com_content&task=view&id=200&Itemid=84

Carrier, B. D. (2006). A Hypothesis-based Approach to Digital Forensic Investigations. CERIAS Tech Report 2006-06, Purdue University, Center for Education and Research in Information Assurance and Security, West Lafayette.

Dafiri, S. (2003), In-Depth Studying of The Law on Criminal Procedure in Saudi Arabia, Dar Tibah, Riyadh.

Elguindy M, (2012), Cybercrime Challenges in Middle East. http://www.academia.edu/5022865/Cybercrime_Challenges_in_Middle_East.

Farid, Z. (2017). What is the hadith and sunnah?. [online] Quora. Available at: https://www.quora.com/What-is-the-hadith-and-sunnah [Accessed 6 Aug. 2018].

Fisher, M.P., 1997. Living Religions: An Encyclopaedia of the World's Faiths. IB Tauris.

Hadith Commentary. (2013). Hadith 32. No harming nor reciprocating harm. Available: https://hadithcommentary.wordpress.com/nawawi/hadith32/. Last accessed 22 NOV 2017.

Madkoar, M.S. (1980). The Effect of Islamic Legislation on Crime Prevention in Saudi Arabia. Ministry of Interior, Kingdom of Saudi Arabia, (In Arabic).

Muhammad Farooq-i-Azam Malik (2001). Al-Qur'an, the Guidance for Mankind - English Translation of the Meanings of Al-Qur'an with Arabic. U.S: The Institute of Islamic Knowledge. 691-692.

Muhammad Saalih al-Munajjid. (2016). Is there a difference between the Hadeeth and the Sunnah. Retrieved from https://islamqa.info/ar/145520.

Imam Nawawi's Forty Hadith: Hadith 32, 33, and 34: Do not harm, Burden of proof, Resisting evil. Retrieved from http://bible-Qur'an.com/islam-hadiths-hadiths-32-34-nawawi/.

Islamweb. (2009). Morality in Islam. Retrieved from http://www.islamweb.net/en/article/134385/morality-in-islam.

Perumal, S. (2009). Digital forensic model based on Malaysian investigation process. International Journal of Computer Science and Network Security, 9(8), 38-44.

Qur'an. Translation to English Available at: http://quran.ksu.edu.sa/translations/english/

Stamatel and Sung, (2010), Crime and Punishment around the World, ABC-CLIO ISBN: 978-0313351334

Studies and Research Department. (2013), Claims of cybercrimes and evidence proof in the Arab legislations between reality and expectations. Retrieved from

http://www.carjj.org/sites/default/files/%D8%AF%D8%B9%D8%A7%D9%88%D9%89%20%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85%20%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9%20-%20%D8%A7%D9%84%D8%B3%D8%B9%D9%88%D8%AF%D9%8A%D8%A9.docx

UK Government, Computer Misuse Act 1990, https://www.legislation.gov.uk/ukpga/1990/18/contents

Wathakker.info. (2012). The Most Beautiful Names belong to Allah. Retrieved from http://en.islamway.net/article/12715/the-most-beautiful-names-belong-to-allah.

Wiechman, D.J., Kendall, J.D., & Azarian, M.K. (1994). Islamic Law Myths and Realities. University of Illinois.

