Is a Shari'ah-based Law Compatible with Cybercrime? An Inquiry into the Saudi Regulations on Internet Fraud

Abdullah Faze Algarni
Department of Criminology, College of Social Sciences, the University of Hull

This paper provides a detailed analysis of Saudi regulations on Internet fraud. It begins with an overview of the Islamic Shari'ah’s general stance on fraudulent behaviours, to examine whether it provides a basis for action on Internet fraud. This is followed by a review of the Anti-Cybercrime Act, which was introduced recently to address Internet fraud as well as other forms of information technology-related illicit activity. Other laws considered of particular relevance to the issue of Internet fraud in Saudi Arabia are also examined, to evaluate the extent to which each of them addresses certain aspects of this crime.

Introduction

Internet fraud, along with other forms of cybercriminal activity, has become the subject of a growing concern in recent years in Saudi Arabia. Most of the variants of Internet fraud appear to have found their way into Saudi society. However, a considerable number of those who become victims of online deceptive scams still do not consider reporting their experiences to law enforcement agencies. This, in many cases, is due to the prevalent perception that cybercrime is not a punishable offence in Saudi Arabia (Algarni, 2006). This brings to the fore the legal mechanisms for control of Internet fraud.

Until recently, Saudi Arabia did not have any specific law designed to address Internet crimes or any other kind of computer-related criminal activities. In February 2007, as a result of mounting pressure on the Saudi government by various concerned parties to shape new legislation and legal definitions for cybercrime, the Council of Ministers approved the Anti-Cybercrime Act. The enactment of the new law has been hailed by many Saudi specialists from both the legal and law enforcement sectors as a significant step towards protecting Saudi society from the growing threat of Internet fraud and other criminal behaviours conducted in the virtual world. The legislation, although introduced to deal with a modern phenomenon, is mainly based on the basic principles of Islamic law. Article Seven of the Basic System of Governance in Saudi Arabia, introduced by the late King Fahad Ibn Abdulaziz in March 1992, reaffirms Islamic Shari'ah (Islamic Religious Law) as the foundation of the Kingdom, stating that the government draws its authority from the Holy Qura'an and the Sunnah (Prophet Mohammad's traditions and sayings), and that these two sources govern all administrative regulations of the state. It emphasizes that the state’s role and objective is to protect the principles of Islam and to enforce its Shari'ah. Islamic law, thus, forms the basis for the country’s legal code, and all laws and regulations must be made in accordance with its general rules.

---

This paper seeks to present a detailed analysis of the Saudi regulations on Internet fraud. The fact that Saudi Arabia is governed by Shari'ah (Islamic Law) requires that such an analysis provide an overview of the Shari'ah's general stance on fraudulent and deceptive behaviours, to examine whether it offers a basis for action on Internet fraud. This is followed by a review of the Anti-Cybercrime Act, which was introduced recently to address Internet fraud as well as other forms of information technology-related illicit activity. Other laws considered of particular relevance to the issue of Internet fraud in Saudi Arabia are also examined, to evaluate the extent to which each law addresses certain aspects of this type of crime. Before attempting to do so, however, it is necessary to start by considering the meaning of the concept of Internet fraud and the range and variety of fraudulent schemes committed online.

Definition and Types of Internet fraud

In legal terms, fraud can be defined as “a false representation by means of a statement or conduct made knowingly or recklessly in order to gain material advantage” (Martin, 2003: 211). Fraudsters thus separate victims from their money or property by recourse to misinformation and deception. One may be deceived as to the true value of something that one is purchasing, as to its authenticity, as to its actual owner, and so on. One may also be deceived as to who the individual is with whom one does business, as they may fraudulently present themselves as someone else, such as representatives of some legitimate organisation or the holder of some occupational or professional role to which they in fact have no claim. The deception furnishes the critical tool with which victims are induced voluntarily to part with their money or goods as opposed to being compelled to do so, as in instances of crimes of force (Yar, 2006).

Internet fraud is equivalent to the traditional form of fraud in that it incorporates deceptive behaviour (Grazioli and Jarvenpaa, 2003) that causes financial damage to innocent people. However, although Internet fraud has similar general characteristics to traditional fraud, in being reorganized into the virtual environment it is fundamentally transformed (Cohen, 2002). The nature of this transformation depends on what particular features of the internet are exploited. The Internet is used by both those with an interest in efficient exercises of ‘traditional’ criminality as well as by those familiar with the possibilities of altogether new forms of criminality (Grabosky, 2000). Internet fraud has characteristics that are completely different to those of traditional fraud being, for example, impersonal, anonymous, instantaneous, accessible, and convenient.

Although there is a plethora of labels that began to be attached to fraud once computing technology became involved, definitions of Internet fraud as one specific form of cyber-crime are rarely available in the existing literature. Usually, Internet fraud is defined under the general umbrella of cyber-crime. At the 10th United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cyber-crime was broadly defined as “any

---

2 There numerous terms including computer abuse, computer-related fraud, high-tech fraud, Internet fraud, online fraud, as well as the more recent cyber-fraud (see, for example, Wall, 2001; 2002; 2003; 2008; McQuade, 2006; Yar, 2006; Berg, 2008; Cukier and Levin, 2008).
illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network” (United Nations, 2000: 5). Thomas and Loader (2000: 3) also proposed a definition for cybercrime as those “computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks”. One of the rare attempts to provide a definition of Internet fraud is made by Williams (2000 cited in Chung, 2008: 37). According to William, Internet fraud is “any act of dishonesty or deception carried out with the use of the internet, or directed at the technologies that support the internet “. A solid working definition, which has increasingly been accepted by a significant number of law enforcement agencies around the globe, is provided by the US Federal Bureau of Investigation (FBI) (2003: unpaginated). The FBI describes Internet fraud as:

any fraudulent scheme in which one or more components of the Internet, such as Web sites, chat rooms, and e-mail, play a significant role in offering non-existent goods or services to consumers, communicating false or fraudulent representations about the schemes to consumers, or transmitting victims’ funds, access devices, or other items of value to the control of the scheme’s perpetrators.

Consistent with the above definition, the legal dictionary of The Free Dictionary website by Farlex, defines Internet fraud as:

a crime in which the perpetrator develops a scheme using one or more elements of the internet to deprive a person of property or any interest, estate, or right by a false representation of a matter of fact, whether by providing misleading information or by concealment of information[^3].

It is evident that it is difficult to narrowly define Internet fraud, but with a broad idea of its characteristics, different types of Internet fraud can be distinguished. These misleading activities fall into six categories, as follows: online auction frauds, investment frauds, deceptive advertisement of products and services, advanced fee frauds, phishing and spoofing, and card-not-present payment frauds. While providing extensive details on these forms is beyond the scope of this paper, a brief description of each type can be given. Online auction frauds refer to the deceptive activity committed via auction websites, eBay being the most famous one. These activities can take the form of non-delivery of items; the sale of goods that have in some sense been misrepresented on the auction site; the practice known as ‘shill bidding’, whereby sellers place false bids in order to artificially force up the price of the item, so as to maximise the money that can be extracted from legitimate bidders; and ‘fee stacking’, where the seller adds on additional fees after the auction has been completed, thereby increasing the agreed price for the item (Wall, 2008). As for

investment frauds, 'work at home' and 'stock investment' scams as well as share market manipulation are typical examples of how fraudsters have taken advantage of the instantaneous and wide-access marketing feature of the Internet (Yar, 2006). Deceptive advertisement of products and services are scams that purport to sell goods at greatly reduced prices to hook the victims (Hall, 2005). Some simply fail to deliver the goods or services paid for, or supply them in a lower quality (Grabosky et al., 2001), while others exploit grey markets created by price differentials across jurisdictions or by legal arbitrage where goods that are illicit or restricted in one jurisdiction are purchased from jurisdictions where they are legal (see Granovsky, 2002). Internet advanced fee frauds are online variant of the famous 419 Nigerian scams, in which the target is persuaded to advance sums of money in the hope of realizing a significantly larger gain (see, for example, Edelson, 2003; Holt and Graves, 2007; King and Thomas, 2008). One of the most recent types of Internet fraud takes the form of bogus emails and websites intended to induce victims to voluntarily disclose passwords and other details that can then be used to access their bank and credit card accounts. These take two forms which are usually used in combination to perpetrate the fraud: ‘phishing’ for information via e-mails, and ‘spoofing’ via bogus versions of legitimate financial services websites (Yar, 2006). Finally, card-not-present payment frauds are payment frauds using legitimate credit cards obtained fraudulently via identity theft, account take-over, or fake cards obtained by counterfeiting or cloning information (Wall, 2008).

Having mapped out the terrain of Internet fraud and its various forms, the discussion now turns to focus on the Saudi regulation of these illicit activities, beginning with an overview of the Shari'ah's general stance on Internet fraud.

Internet Fraud from the Islamic Criminal Law Perspective

Islamic criminal law is a part of the general Islamic law, the Shari'ah, which is conceived as a divine law as it comes from, and involves all the authority of, Allah Almighty. Consequently, the state in Islam must be governed according to God's law and the ruler is the executor entrusted with applying God's law.

In Islam, the basis of law is the Glorious Qura'an and the Sunnah. The Qura'an is the words of Allah that were revealed in stages during the lifetime of the last prophet, Mohammad (peace and blessing be upon him), under various circumstances through the Angel Gabriel, while Sunnah means the prophet Mohammad's (peace and blessing be upon him) sayings, actions and the actions done with his approval (Ansary, 2008). The Qura'an and Sunnah, referred to by Muslim jurists as al-Qatiyat (decisive commands based on textual evidence), are considered the fundamental sources of legality, which are unanimously accepted by Muslim scholars. There are, however, secondary sources which can be used when new circumstances arise which were not known in the past. These secondary sources come under the title of Al-ljithad (the striving of a legitimate scholar to reach a religious verdict), which includes mainly consensus (Ijma'a) and analogy (Qiyas). Consensus (Ijma'a), which means the unanimous agreement of religious scholars (Ulama) on a legal judgement at any time after the death of the Prophet, is used by Muslims to settle an issue that has not been provided for in the Qura'an or Sunnah. The general consensus decision
can be accepted as long as it does not contradict the provisions of the Qura'an and Sunnah (Sidahmad, 1995; Vogel, 2000). The issue of analogy (Qiyas) means that if the previous sources fail to provide a rule to address an issue, legal reasoning can be used to solve this problem, by establishing similarity (in the case and in the intention of the law) to an issue on which a ruling does exist. For example, drugs are not mentioned either in the Qura'an nor the Sunnah. However, religious scholars (Ulama) hold that the same legal basis exists as for alcohol, which is prohibited in both the Qura'an and Sunnah, that basis being the deactivation of the mind, and so drugs are also forbidden in Shari'ah. In the area of crime and punishment, the use of Qiyas is permissible. In general, its application as a source of Islamic legislation is considered sound in all injunctions that relate to criminal procedures or criminal policy (Mahmansani, 1952).

Shari'ah law is holistic or eclectic in its approach to guiding individuals on most daily matters. Shari'ah law controls, rules and regulates all public and private behaviour (Wiechman et al., 1994). The rationale of Islamic law is to protect the five important indispensables in Islam: Religion, Life, Intellect, Offspring and Property. Any deviation from or attack on these aspects constitutes crime. Based on such understanding, Islamic law has provided a worldly punishment in addition to that in the hereafter (Madkoar, 1980). Islam has, in fact, adopted two courses for the preservation of these five indispensables: first, through cultivating religious consciousness in the human soul and the awakening of human awareness through moral education; second, by inflicting deterrent punishment, which is the basis of the Islamic criminal system. Therefore, the Hudud, Qisas and Al-Tazir punishments have been prescribed according to the type of the crime committed.

The word Al-Had, the singular of Hudud, in its terminological context, is applied to imply prescribed penalties on certain determinate crimes. These crimes, which are the most serious crimes in Shari'ah law, are apostasy, revolt (the defection of a powerful faction from compliance with the ruling head or chief executive), theft, adultery, defamation (or false accusation of adultery or fornication), forced robbery and consumption of intoxicants. The second category of crimes in Islam is crimes involving human life. This category of crimes implies offences that affect the human soul – murders, injuries and bloodshed. Ulama refer to this category with new terminology – crimes of Qisas and al-Diyyat. Qisas is a prescribed penalty for intentional offences – murder or injuries. A crime of Qisas is one for which the victim has a right to seek retribution and retaliation (Al-Zuhaili, 1984). According to Al-Ali (2007), the concept of retribution was found in the first statutory Code of Hammurabi and in the law of Moses in the form of ‘an eye for an eye’. Muslims add to that saying, “but it is better to forgive.” (Ibid: 6). Crimes of al-Diyyat, on the other hand, are those carried out by the perpetrator with no intent, in absolute terms, to kill the victim. Diya, the singular of al-Diyyat, is ransom money paid by the offender to the victim if he/she is alive. If the victim is dead, the money is paid to the victim's family or to the victim's clan or tribe. The assumption is that victims will be compensated for their loss. Diyah, however, can be enforced on the criminal in crimes of Qisas. This is when the victim in cases of physical injury or partial fracture, or the heirs of the victim in murder cases, chooses to accept financial compensation instead of insisting on physical retribution (Busaq and Ahmad, 2005).
The above punishments are prescribed in the Qura'an and Sunnah and therefore the judge has no jurisdiction either to increase or decrease the penalty. By contrast, crimes that are not included in any of the previous categories are penalized through non-prescribed penalties, known as Al-Tazir. This term refers to a host of penalties which the Supreme Law-Giver has ordained and authorized jurists and judges to pronounce through judgement verdicts based on manifold factors – flagrance of crime; adversity of its impact, seriousness of the criminal; and intensity of dangers stemming from the behaviour of the criminal. The process of such judgements includes also a careful review of environmental changes that are distinctive in each phase of human history. Al-Tazir penalty is both flexible and adjustable. It can accommodate elements of severity, leniency, intercession and total expiation. An important point to emphasize here, however, is that even in the domain of Al-Tazir penalties, the judge does not enjoy absolute jurisdiction. His judgement and eventual verdict are governed by guidelines emanating from the basic Islamic sources, the intents implicit in such sources and pertinent objectives. In no event must his judgement be influenced by his personal whims or caprices. Rather, the focus of his consideration should be on the determination of the course which is most adequate and most relevant (Busaq and Ahmad, 2005).

In shedding light on Al-Tazir penalties, a general observation can be made, that such penalties cover a wide spectrum. The most lenient penalty is the mere announcement of the name of the criminal, i.e. 'naming and shaming'. The severest penalty is execution. Jurists have listed penalties that fall in the Al-Tazir category. These include advice and guidance, scolding and admonishing, ostracism, publicity, threats, deprivation, suspension from employment, eradication of crime impact, financial penalties, extradition and exile, prison or detention, flogging, and execution (Ibn Al-Qayyim, 1986).

It is indeed very difficult to count, statistically, the exact number of crimes that are prone to the application of Al-Tazir penalties. Some of such crimes are well known. Others are the products of time and space, emerging with changes in the modern age. In operational terms, the number of Al-Tazir penalties executed, according to Busaq and Ahmad (2005), far exceeds those of other forms of penalties. In fact, it has been estimated at 95 % of all penalties executed.

Based on the previous analysis, Internet fraud is one of the crimes that fall in the discretionary spectrum of the chief executive and judiciary. They are given the right to impose penalties for the crime as they deem appropriate. The determination of the penalties must follow a careful consideration of all factors involved. The ruler is also authorised to amend the penalties in the public interest. The Islamic criminal policy is one which has a responsive approach to each new crisis situation, such as Internet fraud and other forms of information technology-related crime. On this point, the assertion of Ibn Al-Qayyim (a prominent Muslim jurist and philosopher) is noteworthy. He has expressed that "pertinent policy must be commensurate to the exigencies of changing times. Never assume the general laws are rigid invariably for this Ummah (Nation) until the day of Judgement" (1986: 19).

Other top ranking Ulama have expressed similar ideas. In essence, all concur that a flexible approach is the most appropriate response to the variety of issues and multiplicity of problems that emerge with the variance of contextual settings – chronological and situational (Busaq and Ahmad, 2005).
In Spire Journal of Law, Politics and Societies (Vol. 5 No.2 – 2010)

Shari'a’s approach to legislation is guided by an operative rule: ‘No penalty is enforceable without textual evidence’. This rule shows that the legitimacy of crime and its punishment is based on textual evidences of both the Qura'an and Sunnah. The spirit of this rule is expressed in numerous Qura'anic texts. For example, Allah Almighty says:

And We never punish until We have sent a Messenger (to give warning)" (Surah Al-Isra (night travel): verse 15). Allah also says, "And never will your Lord destroy the towns (populations) until he sends to their mothertown a Messenger reciting to them Our Verses (Surah Al-Qisas (stories): verse 59).

Fundamentally, the guiding rule – ‘No penalty is enforceable without textual evidence’ – is applicable to crimes involving Hudud and Qisas penalties. Likewise, the applicability of the above rule is reflected even in Al-Tazir crimes that attract the lightest to the hardest penalty – verbal advice to execution. Al-Ijtihad (the striving of a legitimate scholar to reach a religious verdict) related to such types of penalty requires some textual substantiation (Mahmansani, 1952; Al-Zuhaili, 1984).

With regard to Internet fraud, the textual substantiation needed for the application of Al-Tazir penalty is provided in the Qura'anic verses and Ahadith (Prophet's sayings) prohibiting fraud and deception and criminalizing the acquisition of wealth through unlawful means. To start with the Qura'an, Allah Almighty commands, "O believers! Do not consume one another's wealth through unlawful means; instead, do business with mutual consent" (Surah Alnisa'a (women): verse 29). This text clearly shows that, in Islam, acquiring the property of others is only permitted through fair trade and honest business, with the total consent of both parties. Another verse states, "Give just measure and weight, and do not withhold from the people the things that are their due" (Surah Al-Ara'af: verse 85). More particularly, any attempt to cheat in business transactions is castigated vehemently by Allah Almighty. This is declared expressly in the following verse: “Woe to Al-Mutaffifin (fraudsters), those who, when they have to receive by measure from people, have exact full measure, but when they have to give by measure or weight to people, give less than due” (Surah Al-Mutaffifin: verse 1-3).

Prophet Mohammad (peace and blessing be upon him) also reinforced the prohibition of fraudulent activities and dishonest practices in Muslims' behaviour towards fellow Muslims and non-Muslims equally. In this respect, the Prophet (peace and blessing be upon him) has been reported to have said:

The signs of a hypocrite are three: Whenever he speaks, he tells a lie; Whenever he promises, he always breaks his promise; If you trust him, he proves to be dishonest; If you keep something as a trust with him, he will not return it (Al-Bukhari, 1987: 230).

Also, it was narrated that the Prophet (peace and blessing be upon him) said: "He who cheats us is not one of us" (Al-Nawawe, 2004: 604). The statement means that a cheat does not count as a Muslim, and it explains to what extent Islam has forbidden fraud and cheating. In another statement which carries a
similar meaning, Prophet Mohammad (peace and blessing be upon him) said, “No-one should sell anything without disclosing any defect in that thing and he who knows about this defect is obliged to tell the buyer” (ibid: 605).

It is clear from the preceding texts and statements that Islam prohibits fraud and requires Muslims to be straightforward in all their deeds. Truthfulness, sincerity and honesty are basic ethical values of Islam. As Zainul et al. (2004) argue, there is no scope for cheating, deception and dishonesty in the Islamic framework of human relationships.

In essence, fraud is held to be a form of theft. In Shari'ah law, theft is an offence liable for application of the Had (the singular of Hudud) penalty of hand amputation. The punishment is prescribed in the following Qura'anic text: “Male or female, whoever is guilty of theft, cut off their hand (that was used in theft): A retribution for their deed and exemplary punishment ordained by Allah, and Allah is Exalted in Power, Full of Wisdom” (Surah Al-Ma'aeda: verse 38).

However, to prove the offence of theft, in the legal sense, which ends with a judicial sentence of hand amputation, the act of stealing must be carried out in secrecy, without the prior knowledge and consent of the owner of stolen assets. The items stolen must be regarded as assets or property in the legal sense of the term, have been taken from a safe used for keeping valuables, and be worth at least three Dirhams or a quarter of a Dinar, at the time of the theft. They must belong to someone other than the accused, and the owner must have demanded their return. The thief must be an adult, competent person, acting of his own free will, and with criminal intent. He must not have been forced to steal by hunger; no amputation is imposed during a year of famine or of high living costs. Nor is there amputation if a child steals from his parents. The case must be proven either by the testimony of two trustworthy men or the confession of the culprit.

If one of the above stated conditions is absent, the offence will not be liable for the application of the theft Had of hand amputation. Instead, an Al-Tazir action will be carried out on the offender (Ibn Duyan, 1961; Abu-Hassan, 1987; Al-Mogahem, 1994).

According to these rules, offenders of Internet fraud are not regarded, from the perspective of Islamic criminal law, as thieves, in the legal sense of the term, eligible for the penalty of hand amputation ordained by Allah for theft Had. The reason for this is that some of the above listed conditions can never be met in Internet fraud cases. For instance, it is required that the stealing action is performed without the prior knowledge and the prior consent of the owner of stolen assets. In Internet fraud, however, the stealing act is carried out with the victim being aware of, and in some cases agreeing to, the process leading to the loss of their money. Moreover, Internet fraud does not involve the physical action of stealing a property from its safe; instead, the fraudster utilises tricks and deceptive methods to falsely persuade the victim to part with their money. This takes Internet fraud out of the boundaries of theft Had and renders it, in Shari'ah law, an offence punishable only by an Al-Tazir penalty, which is, as has been previously explained, determined through a process based on juristic-judicial Ijtihad (the striving of a legitimate scholar to reach a religious verdict) of the pertinent scholars and specialists.
From the previous analysis, it can be concluded that Islamic law supports all positive laws and regulations in prohibiting and incriminating fraud and deception, and drives at protecting people's lives and property, besides maintaining public security in a manner that ensures the progress and development of the community. The discretionary penalty system – Al-Tazir – used in the Islamic criminal jurisprudence for such crimes provides an extensive background for Saudi legislators to formulate regulations capable of handling Internet fraud and set adequate punishments to deter its perpetrators. This is reflected in the introduction of the Anti-Cybercrime Act, which has been put forward by the Saudi government to address different types of technology-related criminal activity, Internet fraud being one of the most notable. The next subsection is intended to consider the various provisions in the Saudi Anti-Cybercrime Act relating to Internet fraud in terms of definition, characteristics of the crime and available penalties.

The Anti-Cybercrime Act

Issued under the Council of Ministers resolution No. (74) dated 05/01/1428H (corresponding to 12/03/2007) and approved pursuant to the Royal Decree No. (M/12) dated 12/01/1428H (corresponding to 26/03/2007), the Anti-Cybercrime Act is the Kingdom's first set of laws designed to combat the growing threat of IT crimes. Prior to the introduction of this legislation, judgement in computer crime cases presented before the General Courts, which are ruled by Islamic law, was left, as already explained, to the judge's discretion.

In brief, the Act comprises sixteen articles. Article One provides definitions of the terms used throughout the subsequent articles. The objectives sought through the enactment of the legislation are set out in Article Two. It states that the Act aims at creating legal and regulatory standards to combat information, computer and Internet crimes through specifying/determining the relevant crimes and punitive actions for each crime or violation, in order to achieve the following: "1) maintain information security; 2) safeguard the rights associated with legitimate use of computers and computer networks; 3) protect public interest, morals, and communal values; and 4) develop and safeguard the National Economy".

Articles three to 13 are concerned with identifying punishable cybercrimes and specifying penalties for them. The remaining articles define the duties of the agencies responsible for enforcing the law.

The Anti-Cybercrime Act does not specifically define Internet fraud. However, the broad definition of cybercrime provided in Clause Eight of Article One clearly encompasses Internet fraud as one of the offences which the Act has been created to tackle. It states that a cyber-crime is "any unlawful act that is committed using a computer or the Internet or any other means or device of information technology or the like". By defining cybercrime in such extensively inclusive terms, the Act also provides a safeguard against any new form of cybercrime that might emerge in the future.

It is worth noting, nevertheless, that the specific mentioning of only some violations relating to cyber-fraudulent activity in the Act may seem to cause some confusion in this regard, as it might imply that the Act is not inclusive of all forms of Internet fraud. The specifically mentioned violations are when a person:
1. Takes possession for himself or for a third party, through an information network, a computer, or a similar means, of cash money or a voucher or signing such a voucher utilizing a fraudulent means or a fake identity or impersonation if such an action is meant to deceive the victim.

2. Uses the Information network, a computer, or similar means to access unlawfully and unrightfully bank accounts, credit card information or the like, or to utilize such information to obtain personal data, funds or services (Article Four).

From the Writer's point of view, this constitutes a weakness in the law and opens the door for interpretations which could sometimes be incorrect. The weakness of the Anti-Cybercrime Act with regard to Internet fraud has been emphasized in a review conducted by the Saudi Communication and Information Technology Commission (CITC) to assess how the issue of spam is currently addressed by the existing Saudi legislations. The said review noted that spam messages are not fully dealt with by the newly promulgated Anti-Cybercrime Act and suggested that significant gaps exist in the law's ability to address this as well as other forms of Internet fraudulent activity. For example, the CITC's report has pointed out that while the Anti-Cybercrime Act prohibits certain types of content in electronic messages, it does not explicitly address the issue of unsolicited commercial messages, considered to be a major form of spam. The Act, according to CITC, fails to explicitly define spam and unsolicited commercial advertisements, the nature of the consent required, and requirements for legitimate messaging (CITC, 2007). Spam represents a major annoyance and threat to Internet and communications infrastructure, applications, computer users in general and to users of the Internet in particular. In the Kingdom of Saudi Arabia itself, as was noted in the abovementioned document, spam has been used for malicious purposes including phishing, spreading viruses and fraud. Many regional and international laws have recognised the problem and have therefore included provisions to address the problems and issues that spamming causes. For instance, the recent reform of the UK Fraud Act 2006 Section Two subsections (Two) (Three) creates an offence covering the perpetrators of phishing attacks. The provision is designed to clarify existing laws within the new Fraud Act. A new offence of fraud, designed to reinforce the existing law and simplify the prosecution process highlights the fact that the act of sending such emails without any proof of deception or obtaining of any property will be prosecuted (Savirimuthu and Savirimuthu, 2007). In the United States, Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 was issued to impose limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet. In Section Four of the Act, Chapter 47 of Title 18, United States Code, was amended by adding at the end a new section, Section 1037, which proscribes a penalty of either fine or imprisonment or both for whoever “uses a protected computer to relay or transmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access services, as to the origins of such messages”. Similarly, Pakistan’s Prevention of Electronic Crimes Ordinance, 2007, contains a provision which considers “whoever transmits harmful, fraudulent, misleading or unsolicited electronic messages in bulk to any person without the express permission of the recipient” as committing the offence of spamming (Article 14, Subsection (One)). Subsection (Two) of the same Article declares that the punishment of the offence of spamming will be
fine not exceeding fifty thousand rupees if the offender commits his offence for the first time and for every subsequent commission of offence of spamming he shall be punished with imprisonment of three months or with fine or with both.

While the above and many other anti-cybercrime acts around the world deal with spamming and its issues directly, we find that the Saudi Anti-Cybercrime Act fails to: a) explicitly define spamming; b) stipulate if unsolicited commercial messages can be considered spam; c) state the minimum requirements for legitimate commercial messages, such as the unsubscribe option for users to request the sender not to send such spam anymore; and d) specify the penalties for sending or causing to send unsolicited commercial messages, if this was to be considered spam (CITC, 2007).

On reviewing penalties imposed by the Saudi Anti-Cybercrime Act on those found guilty of Internet fraudulent activity, it is noticed that there are three types of penalties. These are imprisonment, fines and confiscation. The first two of these types are specified in Article Four. The article stipulates that any person who commits the Internet fraudulent activities stated in the article “shall be punished by imprisonment for three years maximum and a fine of no more than SR two million, or either one of them”. Thus, each of these two penalties may be imposed alone or concurrently with the other. The fine is paid to the treasury. A fundamental flaw that has been observed with relation to all penalties involving imprisonment and fines in the Act is that the minimum amount of these penalties is not specified. The Act should define a minimum level for its penalties and not leave it to the personal discretion of the judge, as this might entail the possibility of some sentences not being commensurate with the seriousness of the offence. Confiscation in the Anti-Cybercrime Act is mentioned in Article 13, which calls for the confiscation, in all cases, of all hardware, software and other means used in committing the crimes stipulated in the law as well as the money earned from such unlawful acts. Further, the decision, according to the article, shall include permanent or temporary closure of the site or project, which was the source of the relevant crimes, if the crime is committed with the knowledge of its owner, as determined by the party of jurisdiction, and according to its decision.

Internet crimes involving criminal organizations are given special attention by the Anti-Cybercrime Act. Article Eight states that any person who commits any of the crimes set forth in the Act through a criminal organization shall receive a punishment of no less than half of the maximum amount of the penalty, imprisonment and fines, specified for such a crime. Similarly, holding a public job, with the crime committed during the performance, or as a result, of it; misusing or exploiting minors or the like; and having been indicted, locally or internationally, for similar offences are also conditions considered by the Act as rendering the criminal subject to a punishment no less than half of the maximum penalty (Article Eight). The punishment imposed by the Act on those apprehended after having started, but not finalised, any of the crimes under the law does not exceed, as Article 10 indicates, half the maximum penalty for such a crime. Article 11 of the Act gives the relevant court the right to exempt from the punishments stated in the law offenders who inform the responsible authorities about the crime before it comes to their attention, and before the damage is sustained. However, if the reporting occurred after the crime became known to the authorities, the offender can only be exempted if the reporting helped in
capturing other criminals, if the crime is committed by more than one, or seizing the device used in the crime.

The Anti-Cybercrime Act, however, does not provide well-defined enforcement mechanisms. All that is mentioned in the Act regarding this issue is that "the CITC shall provide support and technical assistance to the responsible security entities during the apprehension, investigation and trial of any crimes under this law" (Article 14). In this context, as the CITC (2007) suggests, the lack of formal coordination mechanisms between relevant regulatory bodies, such as the Ministry of Interior (MOI), represented by the police, and the CITC, and the absence of cybercrime investigation specialists could limit the effectiveness of addressing Internet fraud and other cybercrimes. In addition, the Act did not require the creation of a specialised agency with trained professionals and experts to deal with what are specialty crimes that it aims to address. Such deficiencies in the Anti-Cybercrime Act with regard to the issue of enforcement can hardly be surprising when knowing that the composition of the group that was commissioned to draw the act was not well represented, as it included only lawyers and ICT advisors. Representatives from the police community were omitted, and thus a law enforcement vision was missed in the designing of the newly issued legislation.

Finally, it should be noted that the Anti-Cybercrimes Act is focused on the prosecution of personnel and entities involved in such activities, operating from Saudi Arabia. Accordingly, as with other such laws, it is unlikely that the Anti-Cybercrimes Act will be able to address Internet frauds that might have originated in another country. To be effective, there is a clear indication from cybercrime experts around the world that the harmonisation of laws and the harmonisation of law enforcement practices provide a clearer framework for any effective state-sponsored anti-cybercrime efforts. In an article by Phil Williams, titled "Organized Crime and Cybercrime: Synergies, Trends and Responses", he writes:

Harmonisation is necessary for both substantive and procedural laws. All countries have to reappraise and revise rules of evidence, search and seizure, electronic eavesdropping, and the like to cover digitised information, modern computer and communication systems, and the global nature of the Internet. Greater coordination of procedural laws, therefore, would facilitate cooperation in investigations that cover multiple jurisdictions (2001: unpaginated).

Harmonisation of global and local administrative procedural laws is an essential issue that the Committee designing the Saudi Anti-Cybercrime Act failed to factor into its deliberations. Specific examples of local and international administrative policy and procedural issues can be found in the Saudi Criminal Procedural Code and the Convention on Cybercrime respectively. Surprisingly, the Act did not reference any of the above legal frameworks.

Based on the foregoing analysis, it can be concluded that although the Anti-Cybercrime Act constitutes the main legal reference for controlling Internet fraud in Saudi Arabia, it does not tackle the

---

4 The Saudi police took the initiative in establishing, in 2008, a specialized department, the Informational Crime Unit (ICU), to handle computer crime investigations.
crime in all its detail. Indeed, as shown above, the Act falls short in addressing many aspects of Internet fraud. It is also evident that significant gaps still exist in the law with regard to issues like jurisdiction and enforcement mechanism. Unless these and other gaps are addressed suitably, there are considerable limitations on the Act’s ability to effectively control the activities of Internet fraudsters in Saudi Arabia.

Other Laws Regulating Internet Fraud in the Kingdom

The Anti-Cybercrime Act is not the only law in Saudi Arabia that is considered relevant to the issue of Internet fraud. Two other pieces of legislation contain provisions addressing certain aspects of Internet fraud and, thus, may form, in addition to the Anti-Cybercrime Act, a regulatory framework for controlling this form of electronic crime in Saudi society. These are the Anti-Commercial Fraud Law and the Electronic Transactions Act. The extent to which each of these two laws deals with Internet fraud is examined in what follows.

The Anti-Commercial Fraud Law

According to the Anti-Commercial Fraud Law, every merchant must conduct his trading activities with due diligence, avoiding deeds that involve any kind of scamming, misleading, or cheating of the consumer. The Anti-Commercial Fraud Law provides the Ministry of Commerce (MOC) with the main responsibility for dealing with all forms of consumer-related commercial fraud. The enforcement of this Law, i.e., the detection and investigations of violations of the Anti-Commercial Fraud Law and its Bylaws are mainly the responsibility of the MOC. Moreover, the Anti-Commercial Fraud Law assigns the MOMRA the task of monitoring the expiration dates of foods in the market. As for the enforcement of the Law, six commissions, scattered over different areas in the Kingdom, were set up. A nodal commission, called the National Commission for Consumer Protection, takes the lead and is responsible for leading the various commissions, planning and monitoring the execution, and running consumer protection awareness programme.

According to this law, pecuniary penalties, shutting down the business, imprisonment, and compensation can be applied to anyone who aids, abets or directly commits scamming, misleading, fraud, tricking or cheating consumers regarding the description or advertisement of an item (i.e. misrepresenting the item and misleading or tricking the consumer); the item’s nature, components, types or main features; the item’s origin; and the item’s value, its weight, size, price, etc. It seems that in order to deal with violations regarding the content of the message in fraudulent and misleading Internet advertisements, the Anti-Commercial Fraud Law will be the suitable reference to decide if the content of the message is illegal and consequently invoke actions based on the sanctions provided by the law.

The Electronic Transactions Act

The objectives of the Electronic Transactions Act are to set unified regulatory standards to streamline use of electronic transactions and signatures, and to enhance confidence in the soundness and validity of
electronic transactions, signatures and records. It seeks also to facilitate usage of electronic transactions locally and internationally in fields such as e-government, trading, medicine, education and e-payments. In order to do so, it is intended eliminate barriers in using electronic transactions and signatures, while at the same time preventing misuse of electronic transactions and signatures and related fraud.

Given the nature of the law, there are suitable provisions against specific types of fraud. For instance, the Electronic Transactions Act provides protection against impersonation of another person’s identity, forgery of electronic signatures or digital certificates etc., as well as unauthorised access to systems for the purpose of misusing such certificates (Article 29). Article 30 states that anyone who commits any of the violations indicated above shall be subject to a penalty not exceeding SR five million or five years imprisonment or both penalties. The judgment, the article goes on to mention, may include confiscation of the hardware, systems, software used in the violation and cancellation or suspension of the service provision license. This appears to cover most phishing and related offences, since in all likelihood there will be some form of impersonation of another person’s identity involved.

**Conclusion**

This paper has sought to examine Saudi regulations on Internet fraud, in an attempt to assess the extent to which the Kingdom’s legal system, which is based primarily on Islamic principles, is compatible with new forms of criminality, namely, cybercrime. To achieve this objective, a definition of Internet fraud and its types was first provided. Following that, it was necessary that the discussion give due attention to analysing the Islamic perspective on fraudulent and deceptive activities. The analysis showed that Shari’ah law, which is concerned with protecting property, incriminates those acquiring wealth through unlawful means and imposes penalties on them, but leaves the specification of these penalties to the judgment of rulers and judges. On this basis, Saudi legislators have created a number of laws, which have provisions pertaining to Internet fraud. These laws were reviewed to assess the extent to which they address Internet fraudulent crimes in the Kingdom.

The Anti-Cybercrime Act constitutes the main legal reference for controlling Internet fraud in Saudi Arabia. However, it does not tackle the crime in all its detail. The discussion revealed that the Act falls short in addressing many aspects of Internet fraud. It is also evident that significant gaps still exist in the law with regard to issues like jurisdiction and enforcement mechanism. Unless these and other gaps are addressed suitably, there are considerable limitations on the Act’s ability to effectively control the activities of Internet fraudsters in Saudi Arabia. However, the Anti-Cybercrime Act is not the only law in Saudi Arabia that is considered relevant to the issue of Internet fraud. Two other pieces of legislation, the Anti-Commercial Fraud Law and the Electronic Transactions Act, contain provisions addressing certain aspects of Internet fraud. Thus, the paper has suggested that these laws may form, in addition to the Anti-Cybercrime Act, a regulatory framework for controlling this form of electronic crime in the Saudi society. A concluding remark to be made is that there are two possible legislative approaches in response to Internet fraud: augmentation of existing criminal provisions through amendments; or the creation of new
legislation, whether in the form of an omnibus statute which comprehensively deals with Internet fraud, or specific statutes addressing specific forms of electronically perpetrated frauds. Looking at the latter option, an example can be found in the United States, for instance, where there is a variety of frauds under federal law alone, including identification fraud (18 U.S. Code § 1028), credit card fraud (18 U.S Code § 1029), computer fraud (18 U.S Code § 1030), mail fraud (18 U.S Code § 1341), wire fraud (18 U.S Code § 1343), or financial institution fraud (18 U.S Code § 1344).

References


