International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-4 Number-2 Issue-15 June-2014

Classifications of Cybercrimes-Based Legislations: A Comparative Research between the UK and KSA

Fahad Abdullah Moafa

Abstract

Recent developments in the communications and Information Technology opened wide door on new applications that enable transmitting information accurately and quickly. These developments have of course negative aspects such as enable the cyber predators to conduct their online attacks against the victims. These attacks are called cybercrimes which take many forms. In this paper, cybercrimes in the United Kingdom and Kingdom of Saudi Arabia are highlighted and debated as well as discussing cybercrime types in these countries. Furthermore, this paper depends on the comparison between the UK and KSA legislations to combat the cyber harassments. Where, the UK and KSA legislations were classified according to specific cybercrime types. Moreover, the objective if this research is to improve KSA legislations in terms of combating the new types of cybercrimes appeared based on the UK combating actions.

Keywords

Cybercrime, Cyber-Bullying, Cyber-Stalking, Cyber-Harassment, Cybercrime Legislation

1. Introduction

Internet crimes are increased daily due to increasing the number of internet, it is necessary to protect users' data from these crimes, which take various constitute such as cyberbullying, cyberstalking, and other forms of internet crimes. However, to combat the danger of Internet crimes, it is serious to understand these crimes technically in order to enable the legal people analyze the crime parties, the technologies used, and the crime itself. As it is known for many internet users that, the personal data and other secret data are considered as sensitive information, where the cyberbullying crimes are mainly based on the personal data which are usually used by the cyber predators as it was mentioned by [1, pp. 30–32]. The courts in many countries particularly in Arab world did not establish customized laws to punish the internet criminals against their crimes. Also, the victims lose their rights in these arguments because the legislations do not contain the laws to protect internet crimes. Besides that, these cases need the required technology culture by the investigators and judges.

To understand the cybercrime affects, it is important to review case studies about these crimes from the past experiences of the victims. Where, each case was conducted in specific time and in specific place. However, these case studies aimed to introduce the nature of crime and indicating the punishment law that must be taken for each crime. Moreover, each case identifies the cybercrime properties and the criminal types as well as identifying victim types. Also, these cases showed the nature of crime and indicated where and when the crime had taken place. In addition, the cybercrimes require analyzing all their aspects and analyzing reasons of these crimes. Where, the reasons behind these crimes are often psychological reasons refer to personal features of the criminals, particularly the adolescents' criminals who are trying to have a power over some people (Victims) [1]. Figure one shows the procedures followed in this paper.

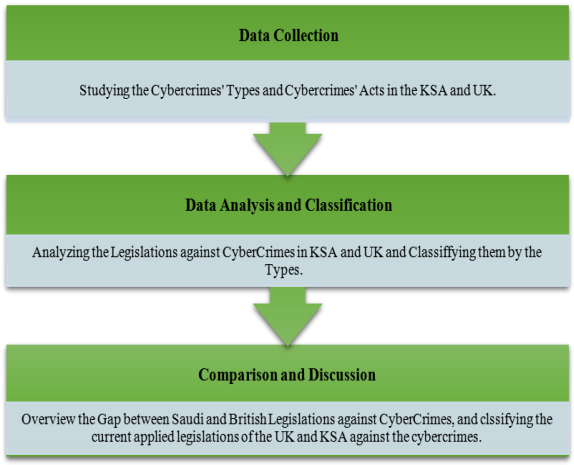

Figure 1: Procedure of Study

Manuscript received June 12, 2014.
Fahad A. Moafa, Institute for Research in Applicable Computing Department, University of Bedfordshire, UK, Information System Ph.D. Researcher.

It is necessary to explain the concept of cybercrime before discuss the legislations against them. Cybercrimes are all threats that take place online through the social networking websites [2]. Moreover, cybercrimes are classified into three types: cyber stalking, cyberbullying, and cyber harassment [3]. In brief, the cyber-stalking can take harassments and reach to cyberbullying in the case when the victim ignores the criminal threats [4]. On the other hand, the criminals of cybercrimes have many objectives behind their crimes such as: getting money, and/or and damaging the reputation of the victims. The cyber predators in most cases use e-mail messages and voice calls at the beginning and then arrive to request money. As a result, the victims are exposed by publishing their personal information or immoral photos and clips, or others.

2. Cybercrime

Cybercrime is defined as a criminal activity including the information technology organization, including illegal access, illegal interception [7] and [5]. Applying traditional criminal concepts to acts involving intangible information can only mean that amendments are unavailable. Many types of cybercrimes were mentioned in previous studies such as: email stealing, hacking accounts, ATM crimes in which the criminal steal the ATM card number and password of the account, in conclusion, the cybercrimes have different types which are mainly classified into three main types as following: cyber-harassment, cyber-bullying, and cyber-stalking [3], [6], and [5].

A. Cyber-Bullying

The cyber-bullying is bullying in which the criminal uses technical means for causing some troubles to the victims. Technical means include electronic devices and equipment such as: smart phones, computers, tablets, etc. Also, cyber-bullying is new method of bullying that had become worry as the technology usage is increased especially by students [2]. Thus, the definition of bullying activities includes effect division, the intent to impose harm and repeated harmful acts. There is an understanding and labeling that has occurred as bullying attempts to be systematically understood, in which there are four different types or facets of bullying. These facets are also known as "methods of attack". These four types of bullying are Oral, Physical (e.g. beating, kicking, and pushing), Verbal (e.g. name calling, abusive language), relational/ social (e.g. spreading rumors, social exclusion). In fact, the technological advances and the rapid growth of communication technology, especially among adolescents, assisted in the transition to a newer version of bullying – cyber-bullying [18]. Where, cyber-bullying is defined as willful and repeated harm inflicted through the medium of electronic communication tools [7].

B. Cyber-Harassment

Harassment is similar to the cyber-bullying in the victim impression about the security levels on the communication tools including GSM networks and Internet websites such as social networking sites. There are many definitions mentioned by various previous researches highlighted the truth of harassment and the tools used by the criminals. As it was defined by [9]. Moreover, harassment can be formed in various ways: sending unwanted, abusive, threatening or obscene e-mails. Also, the harasser can use electronic disruption or spamming, where the victim for example receives a lot of junk e-mail messages. The researcher mentioned that, harassment can also take place in live Internet relay chat sessions. However, online harassment can be indirect which make the mission of detecting the harasser very difficult and complicated process.

Also, cyber-harassment is like physical harassment but its cyberspace is the internet [10]. However, the cyber harassers prefer cyber-harassment because of the suitable cyberspace in which they can conduct harassment without evidence and with inexpensive costs. Where, the victims in both physical harassment and cyber harassment do not record the crimes because of shame and fear attached to the defendant's conduct. It is concluded that, the internet is un-paralleled global communications medium. However, the researchers mentioned that before, the law still has a long way to jurisdictional challenges in a borderless online world. Also, social considerations interact with regularity modalities in cyberspace as in the physical space. These considerations impact and respond to legal and market developments.

C. Cyber Stalking

Stalking, is characteristic in law since the offending behavior is said to occur only when the victim reports themselves to be distressed as a result of the behavior of another whom they believe to be threatening [14]. The victim's insight of the criminal behavior and its effects are therefore pivotal in providing measures on which to make a charge. Therefore, the protection from stalking act states that "a person must not follow a course of conduct which amounts to stalking of

another, and which he knows or ought to know amounts to stalking of the other" "Protect from harassment Act (PfHA), 1997, Section 1) [11]. In parallel, the psychiatric literature has defined stalking as a sequence of behaviours by which one person frequently imposes on another unwanted intrusions to such an extent that the receiver fears for his or her safety [12].

D. Hacking

Hacking related to breaking into others' computers. The internet has opened potentials for hackers to break in without a head physical access to targeted computers. Some hackers hack just to test or boaster their technical skills. Where, some hack to get access to critical data, steal money, or digital possessions, damage data or cause system break downs [13]. Hacking is usually done by the employees who are discontented from their jobs. This may cost the organizations more compensation like stealing information from this organization or steal the account information of the organization and may be it lead to destroy the organization. This crime falls under the consequence of theft, where the primary objective is to steal information [8].

E. Virus Dissemination

Viruses and worms are usually made to destroy data in the computers. It is usually sent by hackers through different approaches such as e-mails, or links to download a program, or video [18].

F. Software Piracy

The copyright infringement of software (Often referred to as software piracy) refers to several performs which include the illegal copying of computer software. Copyright breach of this kind is very common. Most countries have copyright laws which apply to software, but the level of implementation differs There are organizations called Anti-Copyright Infringement Organizations they give the ownerships to copyrighters [15].

3. Cybercrime in the UK and KSA

The recent improvements of Information Technology tools and widespread of communication means in the Middle East, increased the number of Internet users especially in the Kingdom of Saud Arabia. These improvements besides to facilitates introduced by the technical means, provide widespread of the cybercrimes. In fact, the KSA as a big country and youth constitutes, which is considered as the biggest proportion who most of them use the Internet. There were 15.8 million internet users in KSA at the end of 2012 [15] and [16]. Also, there was 54.1% compared to 5% in 2011, as it was mentioned by Communication and Information Technology Commission (CITC). Furthermore, there were 3.6 million people have fallen as victims to cybercrimes in 2012, besides to an average to 195$ indirect financial losses and there were 40% of the country's social networking users have fallen also as victims. As it was mentioned by [16], Saudi Arabia was considered as the most vulnerable of the Gulf countries to fall victims as a result to cybercrimes subject. Also, most Saudi people know about cybercrimes but very less is aware of the associated legislation for combating these crimes.

On the other hand, the UK is a country that suffers from many several cybercrimes happen daily. The UK issued legislations against cybercrimes and these legislations are updated according to the recent cybercrime types that happen in the country [17]. To sense more with the cybercrimes, the home office of UK established a national strategy for cybercrimes. Because of the widespread of cybercrimes in UK, where the home office decided the following: ensuring the compatibility between the work on the national security strategy and cyber security strategy, creating ministerial committee for cybercrime led by ministers from the home office and Business Innovation and Skills (BIS) and reviewing the current legislations across relevant departments considers the influence of cybercrime [18]. On other hand, they recommended to create hostile environment for cyber criminals by learning from the experience of developing Action Fraud and benefiting from the Consumer Direct online reporting facility.

4. Anti-Cybercrime in the UK and KSA

Regarding to cybercrimes in KSA, [15] debated the stand of Saudi Arabian government against cybercrimes and its Information Technology act. Where, the research analyzed the cybercrime in KSA and its associated legislation for combating the same crimes that happened in the UK, taking into considerations the social characteristics of the KSA. Moreover, the research highlighted that there is no clear law in "Shariah" that combat cybercrimes. Because cybercrime form difficult and danger problem to social life, it is serious to establish laws of its own, and be a deterrent to the perpetrator of these

crimes. Furthermore, KSA has a special case that the sanctions imposed as punishment are approved as stated in the Qur'an and Sunnah. All countries' laws have age of children less than 18 years old, but in KSA the children age is less than 15 years old [15]. However, in 2007 KSA established Anticrime act and table 4 shows computer crimes and the proposed Sanctions.

On the other side, UK established legislation to address "Computer Misuse" Act 1990. This law was response to dealing with the increasing crimes of the hackers' in the UK, but there is no clear law against cyber-stalking or cyber-harassment in UK and Wales [11]. The cases that involving in cyber-stalking will fall within the previous of (PfHA) 1997. Where, the overlapping of legal establishment has the great advantage of the flexible supplies of those statutes being able to support proper solutions. Besides that, the civil law can be applied, and this overlapping of statutory provision has the great advantage of the flexible provisions. Nowadays, communications is more fluid so it is necessary engaging existing statutory provisions, in certain circumstances by using electronic media such as email, chartrooms, Facebook, and others. It is possible to say that there is a clear clash between two powerful and important competing rights (privacy) and right to freedom of expression.

In conclusion, the UK legislation did not include the cyber-bullying as independent section yet [5] and [6]. However, it is still subject to laws governing cyber-stalking and menacing and threatening communications such as the Protect from Harassment Act 1997. The government attention focused on applying pressure to technology providers and engaging with the cross-sector members in UK's Council for Child and Internet Safety (UKCCIS). This research recommends establishing new laws to combat cybercrimes by taking into considerations the age of criminals and the environment of crimes.

5. Classifying the Current Applied Legislations of the UK and KSA Toward the Cybercrimes

Specifically, the UK established legislations against cybercrime and against new types of cybercrime such as cyber-bullying law. According to the Computer Misuse law, "the maximum prison sentences specified by the act for each offence were six months, and five years respectively". Where in KSA the law established was against cybercrimes in general in 2007. Therefore, this section aims to classify the UK and KSA legislations against cybercrimes to determine the gap between them. Table 1 shows legislations in UK and KSA against cybercrime.

Table 1: Anti Cybercrime in KSA and UK

No.	Types of Crime	KSA Penalty (Money and Jail)	UK Penalty (Money and Jail)
1	Hacking, Website Defacement Net Extortion.	SR 50,000 or 1 Year or both	18 month prison or £1,000,000
2	Spoofing, Credit Card Fraud.	SR 200,000 or 3 Years or both	Two years prison and £10,000
3	Denial of Service, Software Piracy, Data Diddling.	SR 3,000,000 or 4Years or both	2 years prison Or £1,000,000
4	Virus Dissemination Pornography, Illegal Trade.	SR 3,000,000 or 5 Years or both	18 month prison
5	Cyber Terrorism.	SR 5,000,000 or 10 Years or both	Prison 10 years.
6	Cyber-bullying.	Not defined	Prison between 4 to 10 years and £1,000
7	Cyber-harassment.	Not defined	Not defined
8	Cyber-stalking.	Not defined	Prison between 1 year two 4 years.

6. Discussion

The number of cybercrimes increased significantly in the last decade due to increasing the number of new technologies' users. No enough awareness about cybercrimes for Saudi Arabia internet users especially the youth causes widespread of cybercrimes in KSA. Also, the legislations in Saudi Arabia are not updated about the new types and forms of cybercrimes particularly in the last years. Saudi internet users do not balance between the internet safety and the vulnerability against cybercrime. Most people have knowledge about cybercrimes, but very less people have knowledge about the associated legislation to combat cybercrimes and new types of these crimes. Where,

the UK has better and advanced experiences in establishing legislations against cybercrimes and dealing with the new forms and types of these crimes. Therefore, the classifications-based comparison of this research was for the purpose of encouraging the Department of competing crime in (CPVPV) - KSA to benefit from UK experience in combating cybercrimes by benefiting from the UK legislations in establishing new legislations against cybercrime in KSA, which starts from understanding the nature of the cybercrime technically, then analyse the crime parties, and the technologies used, and finally the crime itself before issuing the penalty.

7. Conclusion

Sharia is the source of legislation in KSA, and most crimes are avoided due to Sharia and fear of God. The cybercrime forms challenge to the Islamic legislations, because there is no clear evidence as well as the cybercrime happens in virtual environment. Thus, the legislation in KSA depends on Islamic Law, therefore the main problem is non-awareness of laws, and the Saudi youth have very little knowledge about cybercrimes and their danger on the society. Also, absence of the evidence forms another challenge to the KSA courts to give justice resolution regarding the cybercrime, where a lack of technical background to understand the nature of the crime technically is considered a main challenge for Department of competing crime in (CPVPV) - KSA. Besides the culture of Saudi people prevent most of victims from reporting their cases especially when they exposure to sexual threats. Moreover, classifying cybercrimes in UK according to legislations used in the courts can be exploited to establish new legislations in KSA against cybercrimes, with taking into considerations the social and religion differences. Applying new legislations in KSA against cybercrimes should improve combating the new types of cybercrimes accordingly.

References

[1] Sveticic, J., A. Milner and D. De Leo, "Suicide research : selected readings", Volume 4, 2010.
[2] McCallion, Gail, and Jody Feder, "Student Bullying: Overview of Research, Federal Initiatives, and Legal Issues", Ongressional Research Service, 2013.
[3] Willard, Nancy, "Cyberbullying and cyberthreats. Eugene", OR: Center for Safe and Responsible Internet Use, 2005.
[4] Cross, Dona, Therese Shaw, Lydia Hearn, Melanie Epstein, Helen Monks, Leanne Lester, and Laura Thomas, "Australian Covert Bullying Prevalence Study (ACBPS)", Child Health Promotion Research Centre, Edith Cowan University, Perth, 2009.
[5] Citron, Danielle Keats, and Mary Anne Franks "Criminalizing Revenge Porn", Wake Forest Law Review, 49, 2014.
[6] Tarapdar, Saima, and Mary Kellett, "Cyberbullying: insights and age-comparison indicators from a youth-led study in England", Child indicators research, 6(3), pp. 461-477, 2013.
[7] Beran, Tanya, and Qing Li, "Cyber-harassment: A study of a new method for an old behavior", journal of educational Computing Research, 32(3), pp. 265-277, 2005.
[8] Sbarbaro, Victor, and Theresa M. Enyeart Smith, "An exploratory study of bullying and cyberbullying behaviors among economically/educationally disadvantaged middle school students", American Journal of Health Studies, 26(3), 2011.
[9] Dadvar, Maral, and Franciska De Jong, "Cyberbullying detection: a step toward a safer Internet yard", In Proceedings of the 21st international conference companion on World Wide Web, pp. 121-126, ACM, 2012.
[10] Lipton, Jacqueline, "Combating cyber-victimization", Berkeley Tech. LJ, 26, pp. 1104–1126, 2011.
[11] Maple, Carsten, Emma Short, Antony Brown, Chris Bryden, and Michael Salter, "Cyberstalking in the UK: Analysis and Recommendations", International Journal of Distributed Systems and Technologies (IJDST), 3(4), pp. 34-51, 2012.
[12] American Psychiatric Association (Ed.), "Diagnostic and statistical manual of mental disorders", 4th ed, American Psychiatric Pub, 2008.
[13] Kim, Won, Ok-Ran Jeong, Chulyun Kim, and Jungmin So, "The dark side of the Internet: Attacks. costs and responses", Information Systems, 36(3), pp. 675-705, 2011.
[14] Mangla, Vikram, and S. N. Panda, "Spectrum of Cyber threats and Available Control Mechanisms", Spectrum, 2(4)., pp. 1439-1447, 2013.
[15] Khan, Naasir Kamaal, "Taxonomy of Cyber Crimes and Legislation in Saudi Arabia", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 1(8), p. 207, 2012.
[16] Elnaim, Bushra Mohamed Elamin, "Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future", In Information and Knowledge Management, 3(12), pp. 14-19, 2013.

[17] Chen, Ying, Yilu Zhou, Sencun Zhu, and Heng Xu, "Detecting offensive language in social media to protect adolescent online safety", In Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom), pp. 71-80, IEEE, 2012.
[18] Britain, Great, "Cyber Crime Strategy", Stationery Office, UK, 2010.

Fahad Abdullah Moafa, born in Sabya - Saudi Arabia, in 10 August 1972. Educational background: B.Sc. Library Science and Information, the University of King Abdulaziz, in Jeddah (1999), M.Sc. Information Science, University of Cairo, Egypt (2007), currently I am a PhD candidate in (Computer System) at the Institute for Research in Applicable Computing Department, in Creative Arts, Technologies and Science School at The University of Bedfordshire - UK, My current position is a lecturer at King Fahd Naval Academy in Jubail, Saudi Arabia, from 2008 (continuously).