REVAMPING CYBERCRIMELAWSIN PAKISTAN : A COMPARATIVE ANALYSIS OF PAKISTAN AND UNITED KINGDOM

by

HAMAISH KHAN

Synopsis submitted to Abdul Wali Khan University Mardanin the partial fulfillment of the requirements for the degree of

LLM

DEPARTMENT OF LAW

DEPARTMENT OF LAW

FACULTY OF SOCIAL SCIENCES

ABDUL WALI KHAN UNIVERSITY MARDAN

SESSION (2022-2024)

REVAMPING CYBERCRIME LAWS IN PAKISTAN: A COMPARATIVE ANALYSIS OF PAKISTAN AND UNITED KINGDOM

BY

HAMAISH KHAN

Registration No. 22031018

Approved by

Supervisory Committee:

_____	
Name: Department Name	Supervisor
_____	
Name: Department Name	Co- Supervisor (if any)
_____	
Name: Department Name	Member
_____	
Name: Department Name	Member
_____	
Name:	Convener, Graduate Studies Committee
_____	
Name:	Convener, Board of Studies
_____	
Name:	Dean, Faculty Name
_____	
Name:	Director, Advanced Studies &Research Board

DEPARTMENT OF LAW
FACULTY OF SOCIAL SCIENCES
ABDUL WALI KHAN UNIVERSITY MARDAN
SESSION (2022-2024)

REVAMPING CYBERCRIME LAWS IN PAKISTAN: A COMPARATIVE ANALYSIS OFPAKISTAN AND UNITED KINGDOM

1. Introduction

In this modern era the global connectivity has touched the horizon and abolished the digital borders across the globe. All the human beings have easy access to the online social platforms, whereby they interact with fellow beings. Similarly, most of the routine manual work is digitalized and put online. At one side it has advanced the daily business, on the other hand all the activities and data remains at risk of cyber-attacks.

A criminal act in which an Android device, window device, a network of computer and a computer is used and targeted for an offence act is termed as cybercrime. It also refers to illegal access to social media, email and similar platforms of an individual or other legal entity. The cybercriminals commit cybercrimes mainly for monetary gain or steal personal information. However, sometimescomputers or networks are damaged by the cybercriminalsfor other than monetary gain motives. Cybercrimes are caused due to various reasons, including lack of security assistance, system vulnerabilities, assessing risks, use of unknown third party applications and software etc. in computers, laptops, android phones and other network devices. Cybercrimes includes fraud of internet and email, fraud of identity, financial theft, theft of data for payment of card, cyber-extortion, cyberstalking, spamming, cyberterrorism, online harassment, child pornography, theft and sale of corporate data, scams of phishing, spoofing of websites, ransomware, malware, hacking of IOT etc.

Cybercrime or electronic crime is a very vast and expanding phenomenon. Cybercrimes across the globe have immensely increased in the past two decades. Numerous cyber-attacks have been witnessed, ranging from developed to under developing countries in the world. Cybercrimes have been witnessed by almost all of the countries around the world. Most of the countries have effected legislation regarding cybersecurity laws.

Pakistan being one of the top populous countries in the world having in use of large internet accessibility. The internet is used almost in all fields, including education, health, defense, research, banking, business, commerce, finance, tax collection, transportation, communication etc. Thus, Pakistan in one of the top countries, fallen prey of cyber-attacks. The Prevention of Electronic Crimes Act, 2016 (PECA, 2016) coupled with Prevention of Electronic Crimes Investigation Rules, 2018 (PECIR, 2018) are the relevant law and rules relating to cybercrimes in Pakistan. This law and rules are applicable to all over the country. The Federal Investigation Agency referred as "FIA" is responsible for implementation of PECA through its Cybercrime Wing.

The United Kingdom is one of the developed countries in the world. Use of internet is backbone of governance system of UK. Being major user of internet UK has also got victim of cyber-attacks. UK has effected very comprehensive legislation relating to cybercrimes. The main codified cybersecurity law is The Computer Misuse Act, 1990 (CMA,1990), while other relevant cybersecurity laws include, the Communication Act 2003, the Malicious Communication Act 1988 (MCA, 1988), Proceeds of Crime Act 2002, the Fraud Act 2006, Forgery and Counterfeiting Act 1981, the Trade Marks Act 1994, Copyright Designs and Patents Act 1988, the Regulation of Investigatory Powers Act 2000 (RIPA), the Data Protection Act 2018, the Investigatory Powers Act 2016 (IPA, 2016), the Network and Information Systems Regulations 2018 (NIS Regulations) and the Privacy and Electronic Communications (EC Directives) Regulations 2003 (PECR). The cyber-attacks and intrusions are mainly investigated by the National Cyber Security Center (NCSC). Other implementation bodies include, UK's National Fraud and Cybercrime Reporting Center, National Crimes Agency (NCA) and Scotland Yards.

This research paper will analyze cybercrimelaws and its implementation mechanism with special reference to Pakistan and United Kingdom. Cybercrimelaws and implementation mechanisms of the UK will be comparatively analyzed with cybersecurity laws and implementation machinery of Pakistan. Major deficiencies will be highlighted in cybersecurity laws and its implementation machinery of Pakistan and fruitful suggestions will be provided for codification of cybersecurity laws, its effective implementation and

eradication of cybercrimes in light of comparison of cybersecurity laws and implementation system of UK.

1.1 Statement of the Research Problem

This research paper will focus on the existing legislation of cybercrime laws and its implementation mechanism in Pakistan and United Kingdom. Cybersecurity space of the above mentioned countries will be comparatively analyzed. Deficiencies in the cybersecurity laws and implementation system of Pakistan will be highlighted in comparison with that of UK. It will be discussed that what kind of cybercrimes are committed and how it will be curtailed through proper legislation and fruitful implementation.

1.2 ResearchObjectives

1. To explore the existing cybercrime laws of Pakistan and United Kingdom and to study it comparatively.

2.To find out the implementation mechanism of cybercrimes in Pakistan and United Kingdom.

3. To investigate the deficiencies in implementation mechanism and cybercrime laws of Pakistan with comparison to United Kingdom.

4.Togive suggestionsfor revamping of cybercrime laws in Pakistan, meaningful legislation and implementation in context of Pakistan with comparative study to the United Kingdom.

1.3 Research Questions

1. What are the existing laws with respect to cybercrimes in Pakistan and UK?
2. What are the implementation agencies for execution of cybercrime laws in the mentioned countries?
3. What are the loopholes in existing cybercrime laws and implementation agencies and how it will be revamped for eradication of cybercrimes in Pakistan with comparison to UK?

1.4 Significance of the Study

This research study will have a great significance and relevancy in the modern digitalized and online world. Itwill enable the readers to get knowledge about cybercrimes, cybersecurity laws and grievances agencies. The current cybersecurity laws will be analyzed and a comprehensive plan of action will be suggested for a harmonized legislation in the mentioned countries, coupled with its implementation techniques, especially in Pakistan with comparison to UK. Recommendations will be given for revamping of cybercrime law of Pakistan. At Policy level, it will also benefit the mentioned countries, especially Pakistan for effective legislation and implementation of cybersecurity laws in a better manner.

2. Literature Review

(Lavigne, 2008) The notion 'Cybercrime' initiallycame into surface in famous science fiction novel "Neuromancer", written by Will Gibson in the year 1985. Due to its intermittent use in a variety of contexts, this term gained its entrance in the common lexicon (Jamil, 2006). In addition, Navneet K., stated that a crime is known as any punishable and illegal act by government or industries establishment, out of all of the multifold offences that take place frequently, the most practiced are that which are committed online as cybercrimes,(Navneet, 2018). Cybercrimesare increasing at accelerating momentum across the globe as a result fast growing technology and its use in all walk of daily business ant its vulnerability to online attacks due to weak safeguarding shield.The current implementation strategy, hardware, software and technology adopted by the law enforcement agencies for hunting of hackers, complex investigation and its eradication is outdated and inadequate for curbing novel forms of cybercrimes. Cyber-criminal acts and cyber operations that constitute cyber war has same methods but with different motives and threshold.

(Gordon, & Ford, 2002) For specification of various types of virtual crimes different nomenclature techniques are adopted. The cyber-dependent crime and the cyber enabled-crime are the two explicit terms used by Gordon and Ford for specification of

cybercrimes. The insertion of malicious and mischievous software, denial of service (DDOS), crimes encompassing hacking are cyber-dependent crimes, which are done by using computer or related window device.Online economic and social networking frauds comes under the category of cyber-enabled crimes, as these are preceding sort of crimes, committed in large scale and severity through internet (McGuire & Dowling,2013). Cybercrimes are further specified into three main categories by Navneet: the cybercrimes against persons (malware, computer sabotage, salami attacks, cyber stalking, cyber-defamation, spamming, phishing, email harassment), cybercrimes against property(logic bomb, Trojan horse, unauthorized intrusion, system hacking, cyber-vandalism, cybersquatting, intellectual property crimes) and cybercrimes against organizations (mail bomb, virus attack, denial attack, password theft, hacking) (Navneet, 2018). Smith, categorized cybercrimes as syntactic,semantic and blended (Smith, 2015).

(Huff, Desilets, & Kane, 2010), the exclusively technical and self-replicating that the victim unintentionally open, as mainly noted in ransomware attacks, are the synthetic crimes. Semantic crimes refer to social networking, while amalgamation of both are referred as blended crimes. Sometime the technique encompasses in the amalgamated crimes enumerate the attacker approaching the victim and presenting an answer to a reasonable issue conclusively suitable that the victim on consent gives permission to financial and personal detailsto the hacker.In such situation, the attacker sold the personal details obtained from the victim and also use it in order to commit further online fraud. Virtual economies are at the stake of risk of cybercrimes. Victimization through cybercrimes has gained momentum in the last decade, especially in respect to harass online (Jones, Mitchell, &Finkelhor, 2013).

3. Research Methodology

In this research paper the Qualitative Research Methodology will be applied. The existing cybersecurity laws, rules and regulations of Pakistan and UK will be studied and textually analyzed. Cybercrimes data of FIA, NCSC, NCA, UK's National Fraud and Cybercrime Reporting Center, Scotland Yards and all other relevant agencies will be studied, compiled and analyzed. All the relevant technical and legal texts, books and journals will

be studied in-dept. Relevant research papers of the scholars will also be analyzed and conclusion will be adduced.

References

Gordon & Ford (2002), Cyberterrorism? Computers & Security, 21(7), 636-647.

Huff, Desilets, & Kane (2010), National public survey on white-collar crime, Rockville: National White-collar Crime Ctr.

Investigatory Powers Act 2016 (IPA), UK.

Jamil (2006), Cyber Law, In 50th anniversary celebrations of the Supreme Court of Pakistan International Judicial Conference on (pp. 11-14).

Jones, Mitchell, &Finkelhor (2013), Online harassment in context: Trends from three youth internet safety surveys (2000, 2005, 2010). Psychology of violence, 3(1), 53.

Lavigne (2008),Mirrorshade Women: Feminism and Cyberpunk at the Turn of the Twenty-first Century, Doctoral dissertation, McGill University, Montreal, Canada.

McGuire & Dowling (2013), Cyber-crime: A review of the evidence, Summary of key findings and implications, Home Office Research report, 75.

Navneet (2018),Introduction of cybercrime and its types, International Research Journal of Computer Science, 5(8), 435-439.

Navneet, (2018). Introduction of cybercrime and its types, International Research Journal of Computer Science, 5(8), 435-439.

Prevention of Electronic Crimes Act, 2016, Pakistan.

Prevention of Electronic Crimes Investigation Rules, 2018, Pakistan.

Smith, Cheung & Lau (2015), Introduction: Cybercrime Risks and Responses—Eastern and Western Perspectives, In Cybercrime Risks and Responses (pp. 1-9). London: Palgrave Macmillan.

The Computer Misuse Act, 1990, UK.

The Communication Act 2003, UK.

The Malicious Communication Act 1988, UK.