International Cooperation and Legal Response to Cybercrime in Pakistan

Tansif Ur Rehman
University of Karachi, Pakistan

INTRODUCTION

According to Internet World Stats (IWS), the total number of internet users in in Pakistan during October 2018 were 44,608,065, which is 22.2% of the total population. More than 30 million of Pakistan's 212 million people use the internet via mobile devices (Bytes for All, 2017). The literacy rate of the country is quite low as compared to other countries, i.e., 58 percent (Economic Survey of Pakistan, 2017).

Research studies into cybercrime with regards to the Pakistani context are nominal, as the field is relatively new. Pakistani has a perfect ecosystem regarding cybercrime, as the internet is widely available. Laws regarding cybercrime exist in Pakistan, but are rarely enforced. The respective culprits usually go largely unpunished in Pakistan. Most common types of cybercrime in Pakistan are criminal access, e-fraud and e-forgery, misuse of devices and encryption, cyberstalking, pornography, malicious code, spamming, unauthorized interception, cyberterrorism, attempt and aiding or abetting.

This research focuses on the common patterns of cyber criminals and the required legislation and enforcement of existing laws along with the need of international cooperation to counter global cyber threat.

OBJECTIVES

1. To highlight the main aims of Electronic Transactions Ordinance, 2002.
2. To highlight the formation of National Response Centre for Cyber Crime.
3. To critically analyze the role of Prevention of Electronic Crimes Act, 2016.
4. To highlight the legislation in Pakistan for international cooperation regarding cybercrime.
5. To discuss the legal response to cybercrime in Pakistan.

BACKGROUND

A bill has to be passed by both Houses of Parliament, i.e. the National Assembly and the Senate. Upon a bill's passage through both Houses, it is presented to the President of Pakistan for assent and becomes an Act of Parliament upon receiving such assent. In National Assembly's absence, statutes are promulgated by the President. The President may, if satisfied that circumstances exist which render it necessary to take immediate action, make and promulgate an Ordinance (Sial & Iqbal, 2015).

The respective framework, i.e., Electronic Transactions' Ordinance, 2002 has provided Pakistan with an initial legal backing regarding e-information as well as communication. National Response Centre for Cyber Crime (NR3C) formed in 2007 is another initiative taken by the Government of Pakistan to trace cyber criminals and to counter the internet misuse.

DOI: 10.4018/978-1-5225-9715-5.ch029

While, the National Assembly of Pakistan has passed the draft of Prevention of Electronic Crimes Act, 2016 (PECA) on 13th April, 2016 after making various amendments to it. PECA was drafted as being part of the National Action Plan (NAP), which was developed in response to the December 2014 attack on Army Public School, Peshawar. This attack took life of 150 people (including 132 children) (Khan, 2018). NAP is a 20 points plan for countering terrorism as well as extremism. It was drafted by the National Counter Terrorism Authority and Ministry of Interior. It got approval from the Parliament on December 24, 2014 (Haider, 2014).

Anusha Rahman Khan - Minister of State for Information Technology and Telecommunication of Pakistan and member of the committee for development of 'Prevention of Electronic Crimes Act, 2016' (PECA) admitted in a summarized note that, Pakistan has no such laws before to deal comprehensively with cybercrime. She belongs to Pakistan Muslim League (Nawaz), which is a centre-right conservative party in Pakistan. She also admitted that, criminal justice legal framework is ill equipped as well as inadequate and to resolve the respective threats of the cyber age.

Although, the PECA has been approved and came into system, but there is huge criticism from the opposition and the IT industry. Critics believe it to be harsh, with punishments not fitting the respective crimes. Another problem is the bill's language, as it could be abused by the government as well as law enforcement agencies in Pakistan.

FOCUS OF THE ARTICLE

This article focuses on the role of Prevention of Electronic Crimes Act (2016), legislation in Pakistan for international cooperation regarding cybercrime, as well as the legal response to cybercrime in Pakistan. This research also cites almost all relevant laws relevant to cybercrime, which have been legislated by the governmental body and defines what is illegal in the Pakistani context. This will help to understand the computer-related crime advancement, and how to use it as defined within the premises of law in the Pakistani context.

ELECTRONIC TRANSACTIONS ORDINANCE, 2002

The implementation of Electronic Transactions Ordinance, 2002 (ETO) has placed Pakistan in those few countries who understood the importance of cybercrime legislation in early time and provided imperative guidelines and frameworks which enabled and encourage the IT industry to foster at higher standards and spread of e-commerce in Pakistan. The Electronic Transaction Ordinance is of high importance that is necessary in carrying out proper IT growth and considered as a turning point for the Information and Communication Technology development as well as growth in Pakistani context.

Ordinance's Main Aim

1. Enhanced electronic transactions.
2. Legal and safe trading platforms for sellers as well as buyers.
3. Economic upheaval.
4. Growth in e-commerce and projection of surgical items, sports goods, leather goods, as well as textile products in the international market.