Cyber-Crimes and Cyber Laws of Pakistan: An Overview

Rashida Zahoor[1]* and Naseem Razi[2]

Abstract

Communications have become the most essential and quite an easy as well as fast because of technology advancement. Developing states are also getting the same blessings of computer networks and internet like the developed nations of the world. Besides, such the blessings and curses take place on account of communications in the modern technology. Cyberspace - is the medium of communication on computer networking that is not safe. Criminals use such the technology to commit crimes on cyberspace. Meanwhile the sensitive data and information are hacked to injure the person, organization, society or even a state. These (cybercrimes) and criminal may be prevented by making the sufficient laws in a country. The principle aim of this study is to discuss the cybercrimes and examine the cyber laws in Pakistan. For this purpose, there are three parts of this paper. The first part addresses the cyber-crimes explicitly in Pakistan. The second part is dedicated to the legal framework of cyber laws in the country. While the last but not least part talks about the cyber security strategy of Pakistan.

Key words: Cyber-crime; Cyber law; Cyberspace; Cyber Security; Internet; Pakistan

1. Introduction

In Pakistan, cyber legislation is still in its infancy. While on the other hand, cybercrimes are more frequent in Pakistan (Mohiuddin, 2006). The evolution of computer had been made the human lives very easy. Every human being and each organization have become the dependent on computers. Our daily routine starts with the alarm of our cell phone which is also a form of computer networking. Computers are those gadgets which are used to fulfil our daily tasks (McQuade, 2008). Digital watches, cellular phone, laptops, desktops and electronic household devices are the common examples of computers. In computers, the information and data are stored to be processed for required and desired purposes. Cyberspace is used to process this data and information on computer network and internet (Usman, 2017). This cyberspace like the conventional word, is also a planet for criminals to commit a cybercrime. Criminals enter into cyberspace and interfere with the data of a person or institute. Sometimes, the computers are used as weapons to commit a crime (Kundi et al., 2014,). In both cases, whether a computer is used as a weapon or targeted as a victim, the outcome is known as cybercrime.

1 Department of Law, University of Sahiwal, Pakistan; and International Islamic University Islamabad, Pakistan.

2 Department of Law, International Islamic University, Islamabad, Pakistan.

*)Corresponding Author.
Email: rashidazahoor@uosahiwal.edu.pk

Cybercrime is a vast term that is used in general sense. Such as, if a crime is committed on a computer through internet with the help of a digital device, it will be known as cybercrime (Sharma & Afshar, 2016). In short, the word "cybercrime" is similar to a crime in which computer, internet, advance technology and cyberspace is involved. In 1995, for the first time in history, the term cybercrime was used to denote the crime which were committed with the help of computer. It was also revealed that a cybercrime may be committed with the help of a computer or against a computer or by the mixture of the both (Kundi et al., 2014). Another fact about this type of crime is that it never demands physical presence of offender on the place incident. unlike other crimes that occur in conventional world, digital crimes need only cyberspace to hurt a person or his property (Munir & Gondal, 2017). For example, if a person has his bank account in Pakistan, this bank account may be hacked by a criminal from any part of the world. Similarly, software piracy does not need the physical existence of a criminal.

To control such type of advance crimes; known as cybercrimes; there is a need of strict control. Which is only possible with the help of competent legal framework (Kundi et al., 2014). Cyber laws are those laws which address the issues in cyberspace and deal with criminals in cyber world. Cyber-crimes and Cyber-criminals who interfere with data and information on cyberspace are the subjects of cyber law. The core theme of this paper is to discuss the cyber-crimes which are common in Pakistan and to examine the cyber laws in this regard. Various electronic crimes which are common in Pakistan are not covered under any reasonable enactment. Despite the fact that the existing legislation; Prevention of Electronic Crimes Act, 2016 (PECA) doesn't cover large numbers of the current violations.

2. Cybercrimes in Pakistan

With the advent of internet, 3G/4G technologies and ICTs Pakistan is doing a struggle to make advancements in both, the public and private sectors. The fast advancement of technology is a great danger for countries especially for the developing countries to protect not only individuals and organizations, but also the country itself; from cyber-crimes. Unfortunately, Pakistan is not free from cybercrimes. In fact, cybercrimes are happening more frequently and rapidly in our society (Usman, 2017). Pakistan is currently facing the following types of these crimes:

2.1 Cybercrimes against Individuals

In this type of cybercrimes, the victim is a living person. Examples of such the type of cybercrimes are given below:

2.1.1 Email Spoofing: This crime is committed by sending an email. As it is shown in its name, the email is targeted by sending a frogged email with fake title (Awan & Memon, 2016). The header and source of email is shown legal but in reality, it is a spoof email which is aimed to attract the receiver. The

purpose of this type of crime is to get the information from receiver (Kabay, 2008).

2.1.2 Spamming: This cybercrime was originated in 1990 (Ardhapurkar et al., 2010). The offender sends a bulk of email to the different addresses. This unwanted huge traffic of email blocks the legitimate information to be travelled to some specific person. Spam bot's software is used to commit this crime. Email addresses are collected in large amount by this software and spam messages are forwarded to individuals (Sarmah et al., 2017).

2.1.3 Phishing: Phishing is a cybercrime in which victims are attracted by some message in the name of some institute, company or individual. Usually, Bank account of a person as hacked in this method. Fake lotteries, lucky draws and prize awards are offered to collect the secret passwords and codes from an account holder (Sarmah et al., 2017). A report revealed that the Muddy Water, an advanced persistent threat appeared in 2017, to target the sensitive information in Iraq and Saudi Arabia. Now it is also targeting Pakistan, Turkey, Azerbaijan and Jorden. The main focus of this spear phishing documents are the government, military, telecom and educational institutions (Munir, 2018).

2.1.4 Cyber Defamation: Like conventional defamation, cyber defamation is also committed to injure the reputation of some person or entity. However, in this crime the electronic medium is used to infringe the individuals.

2.1.5 IRC Crime (Internet Relay Chat): In IRC type of crime, the internet is used to arrange online meetings with the different criminals. Online chat rooms are created to hold these meetings (Rao, 2016). New techniques and skills framed to commit cybercrimes as interchanged among criminals. Sometime, these chat rooms are created to attract children by evil paedophiles (Khan, 2013). According to a survey conducted by Google, Pakistan, Egypt, Vietnam, Iran, Morocco, India, Turkey, Philippines, and Poland are amongst the top porn watching countries (Staff, 2015). Children are more prone to become victim of cyber-crime. The reports revealed that the worst child abuse scandal as happened in Kasur, Punjab in which approximately 280 children were sexually abused on camera. Later on, the families of such children were also targeted and disturbed. These children and their families were blackmailed (Islam, 2009).

2.2 Cybercrimes against Property

Computer networks and internet are also used to damage a property. Fake and pirated software are the common examples of these crimes (Jaishankar, Ronel, & Sivakumar, 2013). Online threatening messages for destruction of a property also comes in this ambit. Copyright is a right which protects one's property to be used by others. Usually books, music, software, texts, articles are targeted in

"copyright infringement" cases by getting unauthorized access to other's property. Trademark infringement is also one example of such type of frauds (Atta & Haq, 2019).

2.3 Cyber-crimes against Organization

Organizations are the most targeted prey of Cyber-crimes. Sensitive information and data are stolen by hackers from organizations. Sometime, this data is deleted, altered, destroyed or changed and sometime it is sold to competitors (Rasool, 2015). DOS attacks, email spoofing, email bombing, email spamming, web jacking, web hacking, account hacking and salami attacks are routine frauds against organization (Malik & Islam, 2014). Business entities, hospitals, hotels, universities and banks are the common examples of this prey. Banks are common prey of cyber-crime. It is reported by the Director of Federal Investigation Agency (FIA), retired Cap. Mohammad Shoaib that almost all data from Pakistani banks is hacked. He told that about 8000 account of Pakistani banks are hacked and about 100 cases are under investigation in FIA wing (Dawn, 2018).

2.4 Cyber-crimes Against Society

Cyber-crime is also committed against society in the form of pornography, forgery, web jacking, sharing of unethical material against some faith or religion, and hate speeches (Avais et al., 2014). The liberal and progressive-minded persons from academic circles, religious groups, political masses and literary circles are targeted for close surveillance. Journalists, bloggers, members of civil society and human rights activists are mostly targeted for their liberal approach on social media. A Christian boy was charged with the offence of blasphemy for making a like to the post shared to him on his Facebook account. A woman in along with its two female kids was murdered in Chilas on the revelation of an audio call recording of the slain mother with his male friend (Kamran, 2019).

3. Legislations Regarding Cyberspace Technology in Pakistan

Cyber Law means that branch of law that is designed to take control over the crimes committed through the internet in the cyberspace or through the uses of computer resources. Pakistan has made the following cyber laws till now.

3.1 The Telegraph Act, 1885

However, this Act has become insufficient with the advent of modern technologies, but it is kept intact to enhance the powers of federal and provincial governments to interfere with the people's right to privacy. In the name of public interest, unbridled powers are exercised by government without the intervention of courts. The government may take possession of telegraph in case of public emergency and for the public safety. Anyhow, some penalty is also imposed if someone enters into telegraph offices and interferes with telegraph message unlawfully (The Telegraph Act, 1885).

3.2 Pakistan Telecommunication (Re-organization) Act, 1996

This Act provides that the Telecommunication Authority or Frequency Allocation Board should inform the court about any illegal act regarding telecommunication. The court has the power to issue a warrant for search of such premises where illegality is done, further to seize such equipment as used for crime or to make investigations in this perspective (Pakistan Telecommunication Act, 1996).

3.3 National I.T. Policy and Action Plan, 2000

Pakistan Government adopted its I.T. policy in 2000. The objective of this policy was to make laws dealing with cybercrimes. This policy was adopted after studying UNCITRAL Model Laws and consulting the legislation of various civil and common law countries. While keeping in view the approaches adopted by other countries, the "International Consensus Principals on Electronic Authentication" designed by Internet Law and Policy Forum was deemed good to be followed to make this policy (Mushtaque et al., 2015). I.T. policy and action plan are made to make the data of individuals more secured and to protect the way of E-commerce (National I.T Policy, 2000). This instrument is a milestone to make the cyberspace secure.

3.4 Electronic Transaction Ordinance, 2002

This ordinance was promulgated in September 2002. The main object of this Act was to provide the legal backing to the different transactions made on cyberspace. This Act made the electronic record and signatures legal in the eye of law. Further, this ordinance suggests the Federal Government to make rules for the protection of data and to secure the privacy of the users (Electronic Transaction Ordinance, 2002). However, this ordinance has also many grey areas. It overlooked many crimes which were mentioned in the various international cyber laws of the different countries. It is also the outdated legislation as no update is made in it to meet the speed of new technologies and the new cybercrimes.

3.5 Electronic Crimes Act, 2004

This Act was enacted with the assistance of the ministry of information technology in accordance to the provisions of Electronic Transactions ordinance, 2002. In this Act, the various offences related to the cyberspace were introduced as cyber-crimes. The Criminal access, criminal data access, data damage, system damage, electronic fraud, electronic forgery, misuse of devices, misuse of encryption, malicious code, cyber stalking, spamming, spoofing, unauthorized interception and cyber terrorism were addressed as cybercrimes in this Act (Electronic Crimes Act, 2004). Thus, this Act did not provide any enforcement unit. In addition to this, the acts which were made publishable in this Act that were also not well defined. The definitions of criminal acts were too vague to be understood. This legislation proved useless

without any enforcing mechanisms and because of complexity of language to define the cybercrimes.

3.6 Cyber Security Council Bill, 2014

On 14 April, 2014, a senator- Mushahid Hussain Syed, presented this bill in the senate (Mushtaque et al., 2015). In this bill, it was suggested to constitute a council to deal with cyber security issues at domestic and international level and to draft a 10 to 20 years vision for cyber security along with policies and guidelines. Hence, this bill is not approved till now by Government (Cyber Security Council Bill, 2014).

3.7 The Prevention of Electronic Crimes Act, (PECA) 2016

The bill of this Act was approved in April, 2015, by National Assembly and finally voted by the senate in August, 2017. This Act was enacted after the terrorist attack on Peshawar school. It was adopted as the part of National Action Plan of Pakistan's Government to cater the terrorism in the country. Cyber stalking, cyber spoofing, phishing, cyber harassment, illegal access to an information system or device, illegal access to information or data, illegal interference with an information or data, illegal interference with information system, cyber terrorism, blasphemy and cyber forgery are introduced as cyber-crimes in the Act. However, the language of the Act is not plain and clear. This is the opinion of many human rights organizations and legal experts that language of the act is required to be more specific, and this burliness intervenes into the privacy as well as compromise the freedom of expression (Prevention of Electronic Crimes Act, 2016).

Under this Act, whoever uses the identity of another person to commit any fraud is liable of intrusion into the privacy of a person. The transmission of one's identity information for the purpose to be used in any offence of fraud, deceit or falsehood is also an infringement of the right to a person's privacy. Unlawful interception of any information or hacking of data with the aim to access it or to commit any crime or wrongful gain or wrongful loss or any other like benefit when it is not made public is also an offence. Law enforcing agencies may intercept any information in order to make national security.

Further, the Court may issue a warrant of search and seizer to an investigation officer if it is made satisfied that there exists some data or information which is necessary for investigation. The court may also issue warrant to a person who is in possession of such data resulted from the specified communication to share data within seven days that it believes to be required for the investigation purpose (Prevention of Electronic Crimes Act).

Moreover, the service providers have the authority to retain data for a minimum period of one year that is a clear impediment to the right to privacy and protection of information. Pakistan Telecommunications Authority has the power to remove the contents or block the access to certain information which it thinks to be against the glory of Islam, national interest or security and integrity of Pakistan or injurious to the friendly relations of foreign states,

public interest, ethics, morality and decency. The court may order the real-time collection and recording of such data if it is satisfied by the investigation officer that such data is required for evidence. Furthermore, the investigation officer shall make an application on oath for this purpose. It also authorizes the federal government to share the data gathered from the investigation with foreign intelligence agencies without the intervention of court. It is the discretion of federal government to seize and share such data; however, no internal human right document is highlighted to support these provisions (Sherwani, 2018). Since the passing of this Act several agencies have been empowered to control the individuals and organizations involved in cybercrimes. FIA is empowered to govern the behavior in cyberspace. Funds are to be allocated for the establishment of forensic laboratories and cyber-crime police stations. This Act operates in both ways i.e. to protect the individuals and protect the state. Individuals can seek the justice against crimes like identity or data theft.

To some extent, women are protected in this Act. It provides the protection to a woman against her reputation, any act that amounts to sexual threat, and making her photographs public or using her photograph in the manner to injure her repute (Kundi & Shah, 2009). However, the present Act is not sufficient to secure the privacy of individuals. Hence, this Act is not supported by any updated data protection laws. Similarly, no commission is established to safeguard the privacy and protection of data and information of people.

4. Cyber Security Strategy of Pakistan

Cyberspace has created many dangers to the data and information. This information on the internet and communication systems are needed to be protected from all type of intrusions. It is the obligation of a country to regulate data protection measures. In this regard, the various strategies may be adopted. Laboratories and investigation techniques may also be exercised to highlight the criminals for offences (Usman, 2017).

Pakistan has two response and security measures to deal with privacy issues. One is the National Response Centre for Cyber-crime. The other is Pakistan's Senate Defense Committee (Awan & Memon, 2016).

4.1 National Response Centre for Cyber-crime (NR3C)

To control and counter cybercriminal, Pakistan has established the National Response Center for Cyber-crime (NR3C) to monitor, track and catch the cyber-criminals. NR3C provides education, training and awareness to private individuals as well as organizations and institutions to control and prevent cybercrimes by adopting security measures. It also cooperates with the international institutions and organizations to control crimes originated from Pakistan. It conducts trainings, arranges workshops and seminars for education purpose in the cyber domain. It was found that the advancements in technology brought new threats for data privacy in Pakistan. This center was made to meet

the demands for controlling crimes in cyberspace as people have become more reliant on digital technology which is also not free from cybercrimes. Private and public complaints are addressed in this center. Thus, this center is working only against the offences which are mentioned in the PECA.

4.2 Pakistan's Senate Defense Committee to design the Cyber Security Strategy of Pakistan

After revealing the facts by Edward Snowden that Pakistan has been spied by the U.S. National Security Agency (NSA). It is a dangerous situation for Pakistan to remain the silent and sedentary in making cyber security policy for national security. It was further, revealed by Snowden that US spied on Pakistan's National Telecommunication Corporation (NTC) which is the most important communication channel (Lyon, 2014). This channel is used to communicate between the military and civilian authorities. It is also reported by the Snowden that NSA spied in Pakistan by using a tool known as the SECONDDATE. This tool targeted the FOXACID server of Pakistan and collected all desired information from the computer systems. It is also estimated that about 13.5 billion data has interfered including phone calls, faxes, e-mails (Awan & Memon, 2016).

Senator Mushahid Hussain Syed, the then chairman of the senate committee, arranged a meeting with the Pakistan Information Security Association (PISA), in order to make negotiation for the development of a cyber security strategy. Many discussions were concluded in this meeting. It was suggested that the funds must be allocated for cyber security as it is necessary to protect the cyber-attacks in Pakistan. Seven points Action Plan was discussed by the committee.

4.3 Critical Information Infrastructure Protection

The critical information infrastructure (CII) of a country is the most important property of such the country. The whole economy and the structure of the society is dependent on the frame of this infrastructure. If this system is compromised then, there will be a great threat for the survival of a country. In the case of Pakistan, there is no government department for the safety of any particular CII. No critical infrastructure is declared as the most important infrastructure. No list of C.I.s exists in Pakistan. However, in PECA, 2016, it is mentioned that whoever will interfere with the critical information infrastructures shall be liable to commit a crime. Similarly, it is made more punishable for interferences, alteration, damaging or copying the critical information infrastructures. Further, it is also connected to cyber terrorism. (Awan & Memon, 2016).

4.4 Computer Emergency Response Team (CERT)

Computer Emergency Response Team (CERT) is the composition of highly technical professionals. They are qualified to deal with the cybercrimes. These

people are well equipped to tackle with crimes committed on or by computers and internet and to find out the source of crime.

In Pakistan, it was aimed to make a CERT by the Senate defense committee. This team was among the plans to design a cyber security strategy of the country. But still, there is no CERT in Pakistan. However, the National Response Center for Cyber-crimes (NR3C) is there to deal with these crimes. This center is working to control the cybercrimes in countries. It is also performing the various tasks of CERT as well (Kundi et al., 2014).

5. Analysis of the Discussion

It has been revealed from the above discussion that Pakistan is trying to meet the digital needs of the world. It is the need of the time to become updated in the field of digital technology. It has analysed cybercrimes related to financial matters, Individuals and organizations, such as, advance-fee scam, bank fraud, distributed denial of service attack (DDoS), software piracy, email bombing, email or web spoofing and so on. It is revealed that Pakistan has to take necessary steps for ensuring digital security at all levels. Unlike developed countries, Pakistan has many security threats from cyber criminals. Pakistan is one of those developing countries where the cybercrime is a major problem to be addressed. The major challenges to control these crimes include the inefficient passive defense mechanism, shortage of e-forensic investigation, non-availability of professionals and incompatibility of domestic laws with international laws. Pakistan should design such code of cyber laws which may provide better security measures for national and financial interests. Because of the trans-border nature of cybercrimes, criminals are more privileged to commit these threats (Kundi et al., 2014).

According to a survey, almost 10 to 15 cases are reported on a daily basis related to cyber- crimes involving illegal funds transfer, password cracking, account hacking, salami attacks and internet spoofing (Zaheer, 2018, p. 108). To combat these crimes, Pakistan has made the several laws. However, these laws are not enough to deter criminals from committing cybercrimes. In this regard, no considerable success has been attained to make the cyber environment free from threats (Tubrazy, 2007). Despite of the fact that Pakistan is a signatory of various international instruments, the Government of Pakistan has not designed cyber laws in harmony to the international laws yet

6. Conclusion and Recommendations

With the advent of information and communication technologies; the day-to-day transactions have been shifted to the digital world. From an entertainment to health, education to business; government to military, every sphere of life has become the dependent on internet and technology. Business transactions have been shifted from hype of pages to the digital era. Due to its virtual nature, cyber-crime is the most growing crime in the society. Person and public are not safe from cruses of digital devices. Information and data is the most

fragile subject in cyberspace. From an individual's cell phone to an organization's computer, all are an accessible by offenders. States are also at thread to be intervened by cyber weapons.

In Pakistan, no sufficient laws are there to protect the rights of individuals, institutions, society and states in cyberspace. Therefore, it is the need of hour to deal this cyber giant; so-called cyber-crime; with iron hands. Such type of laws may be designed which can punish the offenders on deterrence perspective. Further, *Pakistan Penal Code, 1860* may also be revised to include the cyber offenses in existing code. Moreover, special cyber laws may also be enacted to protect the institutions. This will help the institutions to safe their information and to build their confidence on customers. Similarly, the sensitive information of state's security matters may also be safeguarded by designing a proper security plan and policy. A team of experts should be there to manage, protect and investigate the cyber issues of individuals, institutions and society.

References

Ardhapurkar, S., Srivastava, T., Sharma, S., Chaurasiya, V., & Vaish, A. (2010). Privacy and data protection in cyberspace in Indian environment. *International Journal of Engineering Science and Technology*, *1*(2), 942–951.

Haq, U., & Atta, Q. (2019). Cyber Security and Analysis of Cyber-Crime Laws to Restrict Cyber Crime in Pakistan. *International Journal of Computer Network & Information Security*, *11*(1), 62-69.

Avais, M. A., Wassan, A., Narejo, H., & Khan, J. (2014). Awareness regarding cyber victimization among students of University of Sindh, Jamshoro. *International Journal of Asian Social Science*, *4*(5), 632-641.

Awan, J., & Memon, S. (2016). Threats of cyber security and challenges for Pakistan. *Proceedings of the 11th International Conference on Cyber Warfare and Security, ICCWS 2016*, (March 2016), 425–430.

Shakeel, Q. (2018, October 23). FIA report on Cyber crime. *Dawn News.*

McQuade III, S. C. (Ed.). (2008). *Encyclopedia Of Cybercrime*, Westport, CT: Greenwood Publishing Group, Inc.

Islam, Z. U., Khan, M. A., & Zubair, M. (2019). Cybercrime and Pakistan. *Global Political Review*, *4*(2), 12-19.

Jaishankar, K., Ronel, N., & SIVAKUMAR, D. (2013). Global Criminology: Crime and Victimization in a Globalized Era (pp. 115–136). New York: Taylor & Francis

Kabay, M. (2008). A Brief History of Computer Crime: An Introduction for Students. Retrieved from: http://www.mekabay.com/overviews/history.pdf

Kamran, A., Arafeen, Q. U., & Shaikh, A. A. (2019). Existing Cyber Laws and Their Role in Legal Aspects of Cybercrime in Pakistan. *International Journal of Cyber-Security and Digital Forensics*, *8*(3), 241-250.

Khan, R. (2013, November 22). Cyber Privacy Issues in India. *SSRN Electronic Journal*, https://doi.org/10.2139/ssrn.2357266

Kundi, G. M., Nawaz, A., & Akhtar, R. (2014). Digital Revolution, Cyber-Crimes And Cyber Legislation : A Challenge To Governments In Developing Countries. *Journal of Information Engineering and Applications*, *4*(4), 61–71.

Kundi, G. M., & Shah, B. (2009). IT in Pakistan: Threats & Opportunities for eBusiness. *The Electronic Journal of Information Systems in Developing Countries*, *36*(1), 1–31.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data and Society*, *1*(2).

Malik, M. S., & Islam, U. (2014). Cybercrime : an emerging threat to the banking sector of Pakistan. *Journal of Financial Crime 26*(1) https://doi.org/10.1108/JFC-11-2017-0118

Mohiuddin, Z. (2006). *Cyber Laws in Pakistan; A situational Analysis and way forward. Islamabad,* Pakistan: Ericsson.

Munir, A., & Gondal, M. T. (2017). Cyber Media and Vulnerability: A discourse on cyber laws and a probe on victimization of cybercrimes in Pakistan. *Global Media Journal: Pakistan Edition*, *10*(2).

Munir, A., & Shabir, G. (2018) Social Media and Cyber Crimes in Pakistan: Facts, Propaganda, Awareness, and Legislation. *Global Political Review, 3*(2), 84-97.

Mushtaque, K., Ahsan, K., Nadeem, A., & Umer, A. (2014). Critical Analysis for Data Privacy Protection in Context of Cyber Laws in Pakistan. *Journal of Basic and Applied Scientific Research*, *4*(10), 1-4

Rasool, S. (2015). Cyber security threat in Pakistan: Causes, Challenges and Way forward. *International Scientific Online Journal, 12*, 21-34.

Rao, K. K. (2016). Human Rights and Cyberspace : Use and Misuse. *Bharati Law Review 12*(2) 5–31.

Sarmah, A., Sarmah, R., & Baruah, A. J. (2017). A brief study on Cyber Crime and Cyber Law ' s of India. *International Research Journal of Engineering and Technology(IRJET)*, *4*(6) 1633-1641.

Sharma, I., & Afshar, M. (2016). Privacy and Freedom Issues in Cyberspace with Reference to Cyber Law. *International Journal of Computer Applications*, *145*(3), 11–18. https://doi.org/10.5120/ijca2016910185

Sherwani, M. M. (2018). *The Right to Privacy under International Law and Islamic Law : A Comparative Legal Analysis*. *1*(1), 30–48.

Staff, P. (2015, January 17). Top 10 Countries That Watch The Most Porn. Retrieved from https://postober.com/2015/01/17/top-10-countries-that-watch-the-most-porn/#

Usman, M. (2017). Cyber Crime: Pakistani Perspective. *Islamabad Law Review*, *1*(3), 18-43,III.

Zaheer, L. (2018). New media technologies and Youth in Pakistan. *Journal of the Research Society of Pakistan, 1*(55), 107–114