Journal of law social and management sciences 4 (1) 21-26, 2025
Journal home page: https://jlsms.org/index.php/jlsms
Open Access
ISSN:2959-3867

A Comparative Study of Cyber Law in India and Pakistan: An Analysis of Legislative Frameworks and Enforcement Mechanisms.

Dr. Naveed Iqbal, *[1] Dr. Hafsa Siddiqui *[2] Dr Abdullah Jumani *[3] Taimoor Ahmed Khan*[4]

*1 Assistant Professor, Mass Communication, University of Karachi
*2 Post doc fellow Islamic Research Institute, International Islamic University Faisal Masjid Campus, Islamabad
*3 Deputy District Attorney Law/ Solicitor,Government of Sindh
*4 Research Scholar, Department of Mass Communication, University of Karachi
Co Email: apro_ku@yahoo.com

Abstract: This research article explores and compares cyber laws in India and Pakistan. As with each passing day crimes are taking a major rise in both the countries. These crimes also include cyber-crimes which is a kind of crime that is committed in the cyber space using computers and internet connection. It does not need the physical presence of the criminal to the place where the crime is being committed. They can do so by sitting at their home using a computer and an internet connection. On a daily basis, the number of cyber-crimes being reported is increasing rapidly in both the countries. There is a big threat to the personal and private information that a person or an institute may possess. The data is manipulated in various ways which may lead to severe loss to the person or the institute owning that data. For this reason, there is a need to secure the cyber space so that these types of crimes may be avoided and a person's private data remains secure. To overcome such crimes and to protect the cyberspace, India and Pakistan have developed cyber laws which are implemented in both the countries. The two neighboring Nations, have evolving legal frameworks which is aimed at regulating cyberspace. In this study legislative measures judicial interpretations and enforcement mechanisms in both the countries relating to Cyber-crimes have been examined. Despite the challenges in combating cyber threats India and Pakistan exhibit different approaches made by their legal systems.
In this analysis key differences and similarities have been highlighted in the scope, efficacy and adaptability of cyber laws. This article shows a deeper understanding of the complicated interaction between law, technology and cyber-crime by comparing the regulatory frameworks. In this research article, cyber laws of India and Pakistan has been compared how community-supported interventions along with digital healthcare systems and legal changes would help reduce these barriers.

Key Words: *crimes, cyber laws, cyberspace,*

INTRODUCTION

The word cyber security has become a catch phrase for the process of controlling every type of Cyber crime which includes identity theft to the development of international digital weapons. Cyber security maybe defined as the gathering of resources, processes and structures to protect cyberspace and cyber space enabled systems from any mishap. Nowadays as there is incredible increase in usage of digital gadgets and internet in both professional and personal life we are more prone to Cyber attacks than ever. It has become a challenge to differentiate between cyberspace and these sectors and to determine the vulnerabilities. Cyber security means protecting sensitive data and systems from online threats. Cyber security measures are also known as information technology (IT) security which works on combating the attacks on network systems and applications. There are two types of cases associated with cybercrime, either the criminal invade the personal data present on the cyber space or they use computer as a weapon for committing a crime. (Kundi et al., 2014,).

Unlike other crimes, cyber crime does not require physical presence of the criminal on the place on incident. (Munir & Gondal, 2017)

LITERATURE REVIEW

Due to a rapid increase in Cybercrimes and cyber threats, there has been a significant evolution in the cyber laws in India and Pakistan. Different legislatives frameworks have been developed by both the countries to combat Cybercrimes.

Cybercrime Evolution and Legislative Response

Cybercrimes were originated when a group named as phreakers emerged in the United States back in 1970s. The group was primarily involved in telephone frauds (Jain & Gupta, 2020). This form of Cybercrime then led to its evolution into more complex cyber threats that we face now. To address these threats, India and Pakistan have taken legislative measures to protect their cyberspace.

Comparative Analysis of Cyber Laws

Information Technology Act 2000 plays a vital role in governing Cyber laws in India (Paul & Aithal, 2018). The IT act legalizes electronic documents and signatures, providing ease in combating Cybercrimes. While cyber laws in Pakistan are based on multiple acts such as Electronic crimes Act 2004 and PECA, dealing with different Cybercrimes.

Challenges and Criticisms

Though, both India and Pakistan have taken measures to combat Cybercrimes by establishing cyber laws, some challenges are still there. For instance, Information Technology Act of India faces criticism for not keeping pace with the rapid evolution in technology (Pajankar, 2020). Similarly, PECA of Pakistan faces criticism because of its complex language and failure to support human rights like freedom of expression and privacy (Mohiuddin, 2006).

Origin of Cyber Crime

In America a group known as phreakers in 1970's appeared and started to get involved in frauds using telephone. John draper was one of the member of this group started to copy the tones used in American telephone and started making free calls. According to some scholars cyber frauds are linked to ARPANET (advanced research project agency network) which is a project that is funded by the US department of Defense.

After sometime the term hacking gained recognition when a group of computer programmers known as phreakers started to attack telephone systems in telecommunications sector. This group started to make free calls and learnt new ways to spoil the system.

INDIA AND CYBER CRIMES

Security, safety, and privacy are crucial for anyone using the internet. Cyber security encompasses the methods, strategies, and processes used to protect computers, programs, networks, and data from unauthorized access, damage, or hacking. India has established strong foundations to protect its population from cyber crimes, prioritizing the best interests of internet users. Cybercrime involves using computers or other electronic devices to target, tool, or store evidence of a crime. Various cyber laws, such as the National Cyber Security Policy and the IT Act, have proven highly effective in preventing unauthorized access. Despite India's stringent anti-cybercrime legislation, the primary challenge remains a lack of public awareness. Those combating cybercrime should anticipate qualitative and quantitative changes in the underlying materials, allowing them to devise strategies that prevent hackers from gaining an advantage.

CYBERLAWS IN INDIA

Since cyber crime is still progressing towards proficiency, no global regulation is there to deal with it (Paul & Aithal, 2018). But the information technology act 2000 has been implemented by the government of India which governs online dangerous and cyber threats. The allotments of IPC and the IT act that outlaw such conduct may coincide sometimes (Lloyd, I. 2020).

Despite of having a broad interpretation, India's current laws cannot extensively deal with all respects of Cyber space activities (Pajankar, S. 2020).

Cyber space activities does not have legal authority or authorization under current laws. For example a big amount of users uses internet for their emails but still email has not been considered legal in India. As there is no formal statute approved by the Parliament, the courts and judges are reluctant to grant judicial legitimacy to email. Therefore, the necessity for cyber law has arise. (Jain, A., & Gupta, N. 2020)

Cyber laws develop a framework to control Cyber crimes and frauds. They offer legal recognition for electronic documents, processing e-filing and e-commerce transactions. Cyber crime deals with every illegal activity which is related to computer, which may include theft, fraud, forgery, defamation and mischief, all of which is covered under the Indian penal code, also the modern crimes which may arise by the misuse of computer, addressed by the information technology act of 2000.

Information Technology Act, 2000

Information technology act 2000 regulates the monitoring, deciphering, and surveillance that relate digital communications in India. According to the section 69 of the IT act, directives can be issued by the central government and state government for monitoring and interception and deciphering of any information communicated received or stored through a computer.

This section of the IT Act expands the grounds for interception compared to the Telegraph Act.

Therefore, Section 69 interception of communications is done in the interest of

• The sovereignty or integrity of India;

• Defense of India;

• Security of India;

• Friendly relations with foreign States;

• Public order;

• Preventing incitement to the commission of any cognizable offense relating to the above; and

• For the investigation of any offense.

The following Act, Rules, and Regulations are covered under cyber laws:

1. Information Technology Act, 2000

2. Information Technology (Certifying Authorities) Rules, 2000

3. Information Technology (Security Procedure) Rules, 2004

4. Information Technology (Certifying Authority) Regulations, 2001

The IT Act is the salient one, guiding the entire Indian legislation to govern cyber crimes rigorously.

Section 43 – (Damage to computer, computer system, etc) Applicable to people who damage the computer systems without permission from the owner. The owner can fully claim compensation for the entire damage in such cases.

Section 43A – (Body corporate failure to protect data)

Section 44(a) – (Failure to furnish document, return or report to the Controller or the Certifying Authority)

Section 44(b) – (Failure to file any return or furnish any information, books, or other documents within the

time specified)

Section 44(c) – (Failure to maintain books of account or records)

Section 45 – (Where no penalty has been separately provided)

Section 46 – (Tampering with Computer source documents)

Section 66 - Applicable in case a person is found to dishonestly or fraudulently commit any act referred to in

section 43. The imprisonment term in such instances can mount up to three years or a fine of up to Rs. 5 lakh.

Section 66 A- Hacking with Computer systems, Data alteration, etc

Section 66B - Incorporates the punishments for fraudulently receiving stolen communication devices or computers, which confirms a probable three years imprisonment. This term can also be topped by an Rs. 1lakh fine, depending upon the severity.

Section 66C - This section scrutinizes the identity thefts related to imposter digital signatures, hacking passwords, or other distinctive identification features. If proven guilty, imprisonment of three years might also be backed by Rs.1 lakh fine.

Section 66 D - This section was inserted on-demand, focusing on punishing cheaters doing impersonation using computer resources.

Section 66 E-Publishing obscene images

Section 66 F - Cyber terrorism

Section 67 - Publishes or transmits unwanted material

Section 67 A - Publishes or transmits sexually explicit

Section 67 B – Abusing Children Online

Section 67 C - Preservation of information by the intermediary

Section 70 - Unauthorized access to the protected system

Section 71 - Misrepresentation to the Controller or the Certifying Authority for obtaining a license or Electronic Signature Certificate

Section 72 - Breach of Confidentiality and Privacy

Section 73 & 74 - Publishing false digital signature certificates

PAKISTAN AND CYBERCRIMES

In the year 1990 the usage of Internet started to increase. Pakistan is one of the top countries when it comes to internet usage. Even though internet has provide us an ease in our daily life it, it has also become a cause of many times such as theft fraud child pornography and extortion. Misuse of internet is increasing day by day in Pakistan, which also involves criminal and unlawful activities. (Mohiuddin, 2006). The usage of Internet increased to approximately 7,7500,000 users by the year 2004 in Pakistan. But at that time Pakistan was lacking a proper framework for investigation of Cyber crime. There was also no sufficient expertise.

Later international response centre for cyber crime was established which was under the control of the Federal investigation agency (FIA) by the government to deal with the cyber crime cases. Specialisation of this agency was in the domain of cyber security cyber fraud technical investigation and digital forensics, and it's goam was to combat the misuse of internet. In the year 2003 the first case of Cyber crime got reported in Pakistan, which involved 5 people which were involved in import export business and were using fake information and misusing credit cards. As per a survey, a total of 10 to 15 cases of cybercrimes are being reported daily in Pakistan. (Zaheer, 2018, p. 108).

As per the FIA reports, In Pakistan, 65% of Cybercrimes are committed on Facebook which involves blackmailing and harassment of women and among these a large number of cases were reported in Karachi. Approximately 20 complaints are received by Karachi cyber wing on a daily basis. Approximately 5500 cases of Cyber crime were reported in Lahore in the year 2018 which involved harassment, blackmailing, stalking, privacy violations, impersonation and fraud.

CYBER LAWS IN PAKISTAN

Electronic transaction ordinance ETO was introduced in the year 2002 in Pakistan. This where the journey of Cyber law and cyber security started in Pakistan. The goal of ETO was to recognize and facilitate the electronic communications and transactions. In 2016 prevention of electronic crimes Act PECA was established, which was a big achievement for the cyber law in Pakistan. PECA extensively dealt with numerous cybercrime issues which involved cyber terrorism, fraud, stalking, and spamming. It also developed various methods and guidelines, for the collection, storage and transmission of electronic evidence. With each passing day cyber crime is taking a major rise in our society. (Usman, 2017)

Legislations Regarding Cyberspace Technology in Pakistan

Cyber law covers legal principles which are developed to government and deal with the crimes that are committed via the Internet in cyber space. Several cyber laws has been established by Pakistan to regulate these activities.

The telegraph act of 1885 is one of those laws, and it is still in affect in Pakistan to date. The aim of the act was to regulate telegraph communications but the act now lacks the advancement in modern technology. According to the act the authorities have a complete power to take the control of telegraph services at the time of public emergencies for the safety of public.

Telegraph Act 1885

Though the telegraph act lacks modern technology, the telegraph act of 1885 continues to strengthen the authority of Federal and professional governments in intervening with people's right to privacy.

In the name of public interest, the government exerts immense authority without judicial supervision. According to the act, the government can seize the control of telegraph services whenever there is a public emergency for the safety of public. The act also applies penalties for any interference with telegraph messages that is unlawful or in case of any unauthorized entry into the telegraph offices.

Pakistan Telecommunication Act

According to the Pakistan telecommunication act of 1996, it is mandatory for the telecommunication authority or frequency allocation board that they must bring into notice of the court if there are any illegal acts that are related to telecommunication. Warrants can be issued by the court in case hosting of any illegal activity is suspected.

National Information Technology Act

The government of Pakistan established its information technology (IT) policy in the year 2000 and the aim of this policy was to create laws which addresses and deals with cyber crimes. The development of this law was followed by the study of UNCITRAL Model Laws and consulting legislation from different civil and common law jurisdictions. Later on "international consensus principles on electronic authentication" was also incorporated by the IT policy which was suggested by the internet law and policy forum.

The goal of IT policy and action plan was to increase the security of data and to protect the framework of e-commerce. This step marks the significant milestone of Pakistan in guaranteeing the security of cyberspace.

Electronic Transaction Ordinance, 2002

In September 2002, The Electronic Transaction Ordinance was declared. The act was intended to provide legal credibility to the transactions occurring online. Electronic records and signatures were legalized by this act, hence, validating them in judicial proceedings. Though the Ordinance had a good preliminary progress, it still possess many limitations. It does not address many crimes that are addressed by international laws of other countries. Also, due to insufficient updates, it fails to keep pace with the rapidly evolving technology, which is the reason behind the law becoming outdated.

Electronic Crimes Act, 2004

The electronic crimes act was established in the year 2004, under the supervision of the Ministry of Information Technology. The act was built upon the facilitation provided by Electronic Transactions Ordinance 2002. Many misconducts regarding cyberspace were introduced by this act and were named as cybercrimes. The offenses include criminal access, criminal data access, data damage, damage to system , electronic fraud, electronic forgery, exploitation of devices, misconduct of encryption, malicious code, cyber stalking, spamming , spoofing, unauthorized interception and cyber terrorism, were all among the misconducts and were addressed under this legislation. (Qureshi,K.N.,&Rohani,M.F. 2020)

Even though the act had a wide scope, it still faced many challenges. No enforcement unit was established for the effective execution of its provisions. Many of its acts were unclear and not properly defined. Moreover, the language used in it was very complex which made it very difficult to prosecute cybercrimes.

This lack of enforcement capabilities called for a need of amendments and improvements in the Electronic Crimes Act to deal with cyber threats for the protection of cyberspace in Pakistan. (Aliero, M., Ghani, 2020).

Cyber Security Council Bill, 2014

Cyber security council bill was presented by senator Mushahid Hussain Sayyed in the Senate on April 14 2014. Establishment of a council tasked with addressing cyber security issues on domestic and international levels was suggested by this bill.

Currently, the bill has not been approved by the government yet.

The Prevention of Electronic Crimes Act, (PECA) 2016

Pakistan's government decided to enact The Prevention of Electronic Crimes Act, 2016, after a tragic terrorist attack took place on a school in Peshawar. The act was approved by National Assembly in April 2015 and then approved by the senate in August 2017. This act is a part of National Action Plan which is developed to counteract terrorism in the country. The act introduced many kinds of cyber-crimes including terrorism, forgery, blasphemy, harassment, phishing, spoofing, and cyber stalking.

Though, the purpose of the act was to combat cyber threats and increase cyber security, the Human rights organization and the legal experts have raised some concerns regarding the language of the act. According to them, the provisions do not have clarity and specificity and may compromise freedom of expression and privacy rights. No internal human rights document is provided to support the provisions of PECA. (Sherwani, 2018)

SUMMARY

Pakistan started its journey of cyber security policy and cyber law in 2002, with the Electronic Transaction Ordinance (ETO), which was intended on facilitating electronic communications and transactions. In 2016, Prevention of Electronic Crimes Act (PECA) was enacted which then became the backbone of framework of cyber law of Pakistan, dealing with a vast range of cybercrimes from cyber stalking to cyber terrorism. But later on, calls of amendment were prompted due to the controversial use of its provisions which were followed by the concerns about human rights violation.

Pakistan has more cyber laws including the Telegraph Act, Pakistan Telecommunication Act, National I.T. Policy and Action Plan, Electronic Transaction Ordinance, Electronic Crimes Act, and the proposed Cyber Security Council Bill.

However in India, Information Technology Act, 2000 governs the judicial framework of their cyberspace. The motive of the act is to fight cybercrimes and regulate cyber activities which it does so by giving legal recognition to e-commerce, facilitate e-filing and developing a legal framework for dealing with cybercrimes. This act deals with various offenses including data breach and privacy violations. By means of IT Act and other regulations, India protects its national security and maintains digital sovereignty.

COMPARING CYBER LAWS IN INDIA AND PAKISTAN:

When comparing the cyber laws of India and Pakistan, following differences and similarities between them can be observed;

Similarities:

1. Legislative Emphasis:

India and Pakistan both have developed specific laws for combating cybercrimes and dealing with cyberspace activities.

2. Electronic Transactions:

Electronic transactions, records, and signatures have been validated legally by the laws of both the countries.

3. Cyber threats:

A wide range of cybercrimes including data breach and privacy violations has been addressed by both India and Pakistan.

Differences:

1. Distinct Legislation:

In India, the major legislation that governs cyber law is the Information Technology Act, 2000.

In Pakistan there are different acts for cyber laws like ECA and PECA.

2. Timelines:

The time of enactment of cyber laws of India and Pakistan are different. For instance, IT Act of India was passed in 2000 while PECA was passed in 2004 in Pakistan.

3. Cyber threats Coverage:

The acts of both the countries deal with different cybercrimes.

CONCLUSION

In conclusion, cyber crime is a kind of crimes that is taking a major rise in both India and Pakistan. With each passing day there is a rapid increase in the number of cases being reported in both the countries. This leads to major loss to the personal and private data owned by a person or an institute. The data is then manipulated in several ways to cause damage to the institute or the person owning the data. Due to this reason, there is a need to protect cyber space in order to avoid such crimes on the cyber space make it a secure place for personal and private data. In order to combat these cyber crimes, India and Pakistan both have developed cyber laws which ensure safety of the cyber space. By comparing cyber laws of both India and Pakistan, it is observed that both the countries have a shared focus on fighting with cybercrimes and regulating activities of cyberspace. There are legislations in both the countries that validate electronic transactions, deals with online misconducts and monitors digital communications. Moreover, there are some differences as well in the implementation of specific laws, and addressing of different crimes.

Regardless of the differences, by following the international standards of cyber laws, a more resilient and integrated response to the cyber threats can be developed in the region.

REFERENCES:

Aliero, M., Ghani, I., Qureshi, K. N., & Rohani, M. F. (2020). An algorithm for detecting SQL injection

awareness, knowledge and behavior: a comparative study. *journal of computer information systems*, 62 (1),

context. *international journal of advanced trends in engineering and technology.(IJATET)*, *3* (1), 59-62.

Jain, A., & Gupta, N. (2020). *Cyber crime. national journal of cyber security law*, *2* (2).

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

Lloyd, I. (2020). Information technology law. oxford university press.

Mohiuddin, Z. (2006). Cyber laws in pakistan; a situational analysis and way forward. islamabad: Ericsson Pakistan (PVT.) LTD. .

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).

Pajankar, S. (2020). Cyber crimes and cyber laws in india. *Delta National Journal Of Multidisciplinary*

Research, 7 (1), 25-29.

Paul, P., & Aithal, P. (2018). Cyber crime: challenges, issues, recommendation and suggestion in indian context. *International journal of advanced trends in engineering and technology.(IJATET)*, *3* (1), 59-62.

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

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