AN ANALYSIS OF DATA PRIVACY AND PROTECTION LAWS IN PAKISTAN

1. MUHAMMAD SOHAIL ASGHAR 2. KASHIF MAHMOOD SAQIB 3. HAMID MUKHTAR 4. HAFSA NAZ

1. Assistant Professor of Law, University of Okara, Punjab, Pakistan email: muhammad.s.asghar@uo.edu.pk
2. Assistant Professor of Law, University of Okara, Punjab, Pakistan email: kashifsaqib11@yahoo.com
3. Assistant Professor of Law, University of Okara, Punjab, Pakistan email: drhamid@uo.edu.pk
4. Visiting Lecturer, University of Okara, Punjab, Pakistan email: hnhafsa777@gmail.com

Abstract-*Revolutionized use of mobile phones, computers, internet and transformation of data from hard to soft form has increased the risks of data vulnerability. Cyber-crimes have proved to be the byproduct of digitalization. Effective cyber-legislation is the only means to monitor, control and prevent these crimes which are being committed by using modern information technologies. Various studies have shown that cyber-crimes are increasing in Pakistan with every passing year due to multiple reasons ranging from insufficient legislation regarding data privacy and protection to lack of cooperation with international law enforcement agencies. This paper examines the most frequently committed cybercrimes in Pakistan, analyzes the existing relevant laws with respect to privacy in general and online data privacy and protection more specifically in order to point out the major challenges in the implementation mechanism and makes a few suggestions to ensure the privacy and protection of cyberspace users in Pakistan.*

Key Words: *Data Privacy, Data Protection, Cyber-crimes, Cyber-legislation, Pakistan*

1. INTRODUCTION

Almost all the segments of contemporary society are reshaped by the modern technological advancements (Heyer, 2007). Data flow was drastically changed in the early nineteenth century with the capability to manipulate electricity (Fang, 1997). During the last few decades, we have attained the ability to gather information by using electrical impulses. The advent of internet has revolutionized the speed of information flow and connectivity has become a matter of just a single click (Weaver, 2019). Political realms globally, including Pakistan, have changed due this digitalization. It has played a vital role in the demise of long-lasting empires of Egypt, Tunisia and many other jurisdictions worldwide (Weaver D. D., 2012). This technological development has caused transition in the commission of crime. In this digital age, most of the crimes are being committed by using the safest mediums such as computer and other electronic gadgets. Real power lies in the information and the lust for it acts as catalyst in the ever-growing rate of cybercrime. Maintaining a database is not such a big task but maintaining its integrity is the real problem (Russell & Weaver, 2012). Not for-profit organizations, governmental and corporate bodies around the globe are much concerned regarding the vulnerability of their huge databases in the absence of any specific stringent law regarding data privacy and protection. Though our lives are much easier now due to the extensive use of information technology but we have to counter specific anomalies, such as unintentional disclosure of data, in the attainment of this object. This involuntary or compulsory disclosure of data could be analyzed from the given illustrations:

1) Whenever we use credit/debit card for shopping, trails of place of shopping and brand preference etc. are left behind.
2) Every person who uses cyber cafes in order to access his mail account, electric trails of his password are stored there unsecured.
3) Websites owners and their allied advertisement companies have the capacity to track our electronic trails, every time we use internet, in order to have access to our choices and preferences.
4) Cyber offenders can easily trace and track the phone call signals of the police in order to have access to their future moves.
5) The whimsical alteration in anyone's account could easily be made by the hackers.

6) Any large-scale organization, using modern equipments and software, could easily track the daily routine and emails etc. of its employees.

It is evident from these illustrations that how easy this is for the cyber criminals to invade our privacy and manipulate our personal data nowadays.

2. CONSTITUTION OF PAKISTAN AND RIGHT TO PRIVACY:

Article 14 of the Constitution of Islamic Republic of Pakistan, 1973 safeguards the right to privacy as a fundamental right of every citizen of Pakistan (Basit, 2015). Pakistan is also signatory of International Covenant on Civil and Political Rights (ICCPR), Article 17 of this covenant (ICCPR ratified, 2010) protects the same. Supreme Court of Pakistan in its numerous judgments, for example in "Benazir Bhutto Vs. President of Pakistan (1997)", recognized and implemented this fundamental right as to privacy and declared that this right has to be protected at any cost if a man is to live with honor and dignity. Article 8 of the Constitution of Islamic Republic of Pakistan, 1973 ensures that all the fundamental rights, including right to privacy, are of paramount importance and no law could be enacted in the country which undermines their dignity (Rana, 2014). In case any law is introduced in contravention of the fundamental rights, such law would be declared null and void to the extent of such contravention. Article 9 & 14 of the constitution also affirm the sacred bond subsists between the privacy of man and his dignity (Shaukat, 2006). Article 4 of the Constitution of Islamic Republic of Pakistan, 1973 enumerates the right to due process of law, clause 2(b) of this Article is directly linked with the privacy of man and protects him against the arbitrary and unlawful interference in this regard. The apex court of Pakistan in "Government of Pakistan and another Vs. Begum Agha Abdul Karim Shorish Kashmiri (1969)" held that all the citizens of Pakistan must be dealt in accordance with law, and nothing but law. life of a person includes not only quantitative but qualitative elements of life which involve but are not limited to privacy of home. The term "home" does not only mean a walled structure where a person resides rather any place where a person enjoys his personal freedom, feels protected against any outside interference and without any fear or vulnerability with reference to his fundamental rights. Right to privacy is the foundation of all liberties, individuality of a person is reliant on letting human exercise privacy related rights. Enormous inter-relation exists between the privacy of a person and his security, this paramount relation is recognized and protected under Article 9 of the Constitution of Islamic Republic of Pakistan, 1973

3. CYBERCRIMES: A THREAT TO DATA PRIVACY AND PROTECTION

A crime which involves a computer or computer network is referred as cybercrime (Moore, 2005), it is termed as computer crime as well (Hadnagy, 2014). We can classify cybercrimes into three broad categories. In the first category computers are used as weapons, online frauds, cyber spoofing, pornography and cyber stalking are its examples. In the second category, computers are utilized as source to store illegally retrieved data. In the third category, computers could be termed as victims, they are targeted in order to steal, modify or destroy the stored data. Privacy breach is becoming a major challenge of digitally revolutionized world. Multiple types of cyber-attacks are being developed rapidly and the privacy of the people around the globe is compromised. Pakistan, being a developing state, is facing more cybercrimes as compared to other developed nations (Usman, 2017). At the moment, Pakistan is facing the following types of cybercrimes:

3.1 Cybercrimes against individuals:

Such crimes are against some specific person rather than the society as a whole. These crimes include but are not limited to email spoofing, spamming, phishing, cyber defamation and internet relay chat. In email spoofing, a frogged mail is sent to the targeted person. The mail seems legitimate from its tile and header/footer of the page but in fact it is a spoof one (Awan & Memon, 2016). The purpose of this cybercrime is to have some information from the receiver (Kabay, 2008). Since its inception in the 1990s (Ardhapurkar, 2010), email spamming is widely used in order to block some important information from traveling from point A to point B. Bulk emails are sent to a number of recipients in this process, spam bots are used to collect email addresses and to forward the spam messages (Samrah , Samrah, & Baruah, 2017).

Another very common cybercrime is cyber defamation; electronic devices are used in the commission of this crime to defame someone. Internet Relay Chat (IRC) is a type of cybercrime whereby criminals are assisted by cybercriminals by providing them online chat rooms to conduct illegal activities (Rao, 2016).

3.2 Cybercrimes against society:

Cyber-crimes are not committed only against individuals, rather against society as a whole as well in the form of web jacking, hate speech, pornography, sharing of material against some specific religion or faith and forgery (Avais, Wassan, Narejo, & Khan, 2014).

3.3 Cybercrimes against property:

Cracked or pirated software (Jaishankar, Ronel , & Sivakumar, 2013) and trademark or copyright infringement (Haq & Atta, 2019) are the examples of such crimes. Threating someone online to destroy his property also falls under this category under the cyber laws of Pakistan.

3.4 Cybercrimes against organizations:

Organizations such as banks, hospitals, hotels and universities in Pakistan are facing cybercrimes in Pakistan. The sensitive data is either stolen, altered or locked by the cybercriminals in order to have ransom or to sell it to someone else for some financial gain or favour (Rasool, 2015). Web/account hacking, DOS attacks, email bombing/spoofing and web jacking are the examples of most frequently used cybercrimes against organizations in Pakistan (Malik & Islam, 2014).

4. AN OVERVIEW OF CYBER LEGISLATION IN PAKISTAN

Cyber legislation in Pakistan is in its initial stages at the moment, we do not have any specific strict laws for the protection and privacy of our data (Mohiuddin, 2006). Pakistani government is struggling to tackle the ever-increasing number of cybercrimes. Government of Pakistan approved “National IT Policy and Action Plan” in 2000 with a view to enact laws relating to cybercrimes and to ensure the privacy users in the cyber space. In order to facilitate online business transactions “Electronic Transaction Ordinance, 2002” was introduced. This Ordinance could not be of much success fundamentally due to the reason that it did not cover all the cybercrimes mentioned under numerous international cyberlaws. Another development in the realm of cyber legislation was made in form of “Electronic Crimes Act, 2004”. Though the Act extended the scope of cybercrimes in Pakistan and made many cybercrimes punishable but the definitions regarding cybercrime and cybercriminal were too vague, further, the Act failed to establish any implementation body or unit, consequently this legislation could not be of much success. Another attempt was made by the government of Pakistan in order to bridge the gap between the cybercrimes and effective legislation and implementation by implementing “Electronic Crimes Ordinance, 2007”. This Ordinance was broadly criticized by multiple organizations mainly because of the vagueness of its definitions and severity of punishment provided for the commission of various cybercrimes.

The most recent cyber legislation in Pakistan is “Pakistan Electronic Crimes Act, 2016” (PECA, 2016). Certain issues regarding online data protection and privacy, such as illegal access of data, utilization of malicious codes and identity theft etc., have been addressed by this Act. Like its predecessors, this legislation has also many critiques from social groups and human rights activists. Certain provisions of this Act authorize the governmental bodies to have access to the personal data of the citizens, such authorization raises serious concerns regarding data protection and privacy in Pakistan.

5. CHALLENGES REGARDING CYBER SECURITY AND DATA PRIVACY

Cybersecurity landscape of Pakistan is facing manifold challenges ranging from lack of competent professionals to deficient defense/enforcement mechanism. The country is vulnerable to cyber attacks such as Gamarue, Peals, Skeeya and Distributed Denial of Services. In 2018 almost all Pakistani banks were cyber attacked and the sensitive data of the customers was stolen (Qarar, 2018). This incident resulted in trust deficit between the banks and the customers.

Existence of terrorist groups in the country is another hurdle pertaining to smooth functioning of cyber laws. Official governmental websites are persistently hacked by the terrorist organizations such as Tehreek-e-Taliban Pakistan (TTP) and Islamic State (IS). These Organizations use these platforms to propagate their anti-state agendas and many innocent people have joined these ban outfits. Bachna Khan University attack (2016) is an obvious example of using ICT where the preparators planned and executed the attacked while sitting in another country (Khan I. A., 2019).

Compromised access to cybercrime awareness concerning data privacy and protection from illegal access formulates another type of cybersecurity threat known as identity theft. Only a few universities countrywide are disseminating cybersecurity related education and trainings but the syllabi goals and scheme of studies are insufficient to redress the existing cyber threats. Moreover, inadequate institutional structure to deal with the challenges relating to cybersecurity annexed with a range of cybersecurity debates with reference to the external threats mostly neglect the cybersecurity challenges faced by the country. The most relevant law i.e; PECA, 2016 is referred as 'draconian' (Khan R. , 2016) as it has granted enormous power to the authorities and most of those powers are misused by the individuals at times (Sridharan, 2016). The said law has failed to differentiate cybercrime from cyberwarfare and cyberterrorism, making punishment too severe or inadequate for the concerned nature of crime.

Lack of support, from the private partners, in order to build more effective and efficient cyberspace infrastructure has also proved a huge challenge for the state consequently it has to rely on the internal investment. Two main organizations responsible for the maintenance of cybersecurity are National Response Centre for the Cyber Crimes (NR3C) and Pakistan Information Security Association (PISA). Despite all the measures taken by the state regarding cybercrime and cybersecurity, we are just in the starting phase as a lot more needs to be done. Week coordination between the military and civilian agencies is another reason for the weak cybersecurity posture of the country.

6. RECOMMENDATIONS

- An all-inclusive cybersecurity policy should be devised by the state whereby all the shortcomings of PECA and in other legislations should be addressed.
- Strict measures must be taken against the concerned government officials involved in the data breach and misuse.
- Strong professional liaison between the military and civilian organization is the need of the hour, combating cybercrime is a multi-dimensional war which requires effective co-operation and co-ordination among all the organs of the state. State must enact such laws which are required to make this liaison effective.
- International co-operation is important to combat cybercrime, an effective mechanism for international co-operation must be devised as the nature of such crimes is global.
- Special tribunals/courts should be established to try cyber cases and trainings for the judicial and legal fraternity be initiated at a large scale in the country.
- Higher Education Commission of Pakistan (HEC) should make it mandatory for all the educational institutions in the country to launch awareness campaigns nationwide concerning cybercrime and cybersecurity.
- State Bank of Pakistan needs to make sure that all the banks in the country are following the global banking standards such as PCI and DSS.

7. THE WAY FORWARD

Cyberthreats are the byproduct of digitalization. Non state actors are constantly breaching the governmental cyberspace in order to fulfil their ulterior motives. Pakistan, being a developing state, is face plethora of cyberspace challenges which need immediate attention from the concerned quarters. Use of ICT by terrorist organizations and organized malicious cyber campaigns against Pakistan by hostile neighboring states are alarming. The policy makers need to enact comprehensive law in order to cater these serious issues of the digital age as the existing law regarding data privacy and protection is insufficient and the implementation mechanism is even weaker, consequently, the personal data at the national level is insecure. We need to transform our reactive cybersecurity approach at the nation level, it should rather be proactive, so that the cybersecurity threats could be accessed in a timely manner and an effective cybersecurity strategy could be devised on time to tackle such threats beforehand.

REFERENCES

[1] Heyer, D. C. (2007). *Communication in History: Technology, Culture, Society*. ThriftBooks-Atlanta.

[2] Fang, I. (1997). *A History of Mass Communication; Six Information Revolutions*. Routledge.

[3] Weaver, R. L. (2019). *From Gutenberg to the internet, Free Speech, Advancing Technology, and the, Implications for Democracy*. Carolina Academic Press.

[4] Weaver, D. D. (2012). *The Right to Privacy in the Light of Media Convergence Perspectives from Three Continents*. Berlin: Hubert & Co. GmbH & Co. KG, Göttingen.

[5] Russell L. Weaver, D. F. (2012). *Protecting Privacy in a Digital Age*. In D. D. Weaver, *The Right to Privacy in the Light of Media Convergence Perspectives from Three Continents*. Hubert & Co. GmbH & Co. KG, Göttingen.

[6] Mohiuddin, Z. (2006). *Cyber Laws in Pakistan; A situational Analysis and way forward*. Global Political Review, Vol. iv No. ii (Spring19)

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

[8] 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.

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

[10] 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.

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

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

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

[14] 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.

[15] 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.

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

[17] 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.

[18] Basit, M. A. (2015). The Constitution of the Islamic Republic of Pakistan with commentary. Federal Law House.

[19] Rana, H. K. (2014). Comparative Constitutional Law. Karachi: Pakistan Law House.

[20] Shaukat, S. M. (2006). Constitution of Islamic Republic of Pakistan 1973. Lahore: Legal Research Centre.

[21] Moore, R. (2005) "Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

[22] Hadnagy, C. (2014). Unmasking the social engineer: The human element of security. John Wiley & Sons.

[23] Qarar, S. (2018). 'Almost all' Pakistani banks hacked in security breach, says FIA cybercrime head. https://www.dawn.com/news/1443970

[24] Khan, I. A. (2019). *Cyber-Warfare: Implications for the National Security of Pakistan*. NDU Journal, 33, 117-132.

[25] Khan, R. (2016, August 11). Cybercrime bill passed by NA: 13 reasons Pakistanis should be

[26] worried. Dawn. https://www.dawn.com/news/1276662