A Critical Analysis of Cyberspace Laws Relating to Right to Privacy in the Light of Socio-Legal Context of Pakistani Society

A DISSERTATION SUBMITTED TO THE DEPARTMENT OF LAW, INTERNATIONAL ISLAMIC UNIVERSITY, ISLAMABAD
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF THE DEGREE OF DOCTOR IN LAWS (PhD LAW)

BY

RASHIDA ZAHOOR
REG # 59-SF/PHDLAW/F14
UNDER THE SUPERVISION OF
Dr. NASEEM RAZI

FACULTY OF SHARIAH AND LAW

INTERNATIONAL ISLAMIC UNIVERSITY ISLAMABAD

APPROVAL SHEET

It is certified that the Viva voce committee has evaluated the PhD thesis of Miss Rashida Zahoor, REG # 59-SF/PHDLAW/F14, titled "A Critical Analysis of Cyberspace Laws Relating to Right to Privacy in the Light of Socio-Legal Context of Pakistani Society", and has conducted her viva voce exam. The committee has found the thesis up to the requirements of International Islamic University, Islamabad in its scope, and quality; therefore, her thesis is approved for the award of PhD degree in Law, FSL, IIUI.

Supervisor
Prof., Dr. Naseem Razi
Associate Professor of Law
Department of Law, FSL., IIUI

External Examiner 1
Dr. Tauseef Iqbal
Assistant Professor of Law
Bahria University, Islamabad

External Examiner 2
Dr. Nadia Khadam
Assistant Professor of Law
Fatima Jinah Women University, Rawalpindi

Internal Examiner
Dr. Ambrin Abbasi
Assistant Professor of Law
Department of Law, FSL.,IIUI

In the name of Allah,
the Most Beneficent,
the Most Merciful

Certificate

The thesis entitled "**A Critical Analysis of Cyberspace Laws Relating to Right to Privacy in the Light of Socio-Legal Context of Pakistani Society**" submitted by **Rashida Zahoor** in partial fulfillment of the requirement of the degree of **"Doctor in Laws (PhD LAW)"** has been completed under my guidance and supervision. I am satisfied with the quality of student's research work and allow her to submit this thesis for further process as per International Islamic University Islamabad rules and regulations.

Date: _____ Signature: _____

Name: _____

DEDICATION

To my parents and those who love Humanity.

DECLARATION

I, Rashida Zahoor, hereby declare that this dissertation is original and has never been presented in any other institution. Moreover, I declare that any secondary information used in this dissertation has been duly acknowledged.

Student: Rashida Zahoor

Signature: _____

Dated: _____

Acknowledgment

In the name of Allah, the Most Gracious and the Most Merciful

Alhamdulillah, all praises to Allah for the strengths and His blessing in completing this thesis. My humblest gratitude to the holy Prophet Muhammad (Peace be upon him) whose way of life has been a continuous guidance for me.

I am deeply indebted to my Supervisor, Prof. Dr. Naseem Razi, for her exemplary guidance and help at every step of my work. She has always been there to provide me with the professional counselling towards the completion of this work. I could not have completed this work without her support and kind directions. It has been a great pleasure and honour to have her as my supervisor.

My deepest gratitude goes to all of my family members. I would like to thank my beloved parents, and also to my sweet sister; Abida Zahoor, for their endless love, prayers and encouragement. Also not forgetting my Husband, Muhammad Yousaf for his love and care. I would sincerely like to thank all my beloved brothers who were with me and support me through thick and thin. Most importantly I would like to thank my little son Muhammad Zohan, whose arrival motivated me to complete this work.

I also want to extend my thanks to Admin Staff in the Faculty of Sharia and Law, International Islamic University Islamabad, for their help and support in the administrative works. I am also grateful to my teachers and friends for motivating me to do PhD (LAW).

To those who indirectly contributed in this research, your kindness means a lot to me. Thank you very much. May Allah Almighty bless them all with His eternal blessings! Ameen.

Rashida Zahoor

List of Acronyms

APCERT	Asia Pacific Computer Emergency Response Unit
APEC	Asia-Pacific Economic Cooperation
ATM	Automated Teller Machine
CCTV	Closed Circuit Television
CDHRI	Cairo Declaration on human rights in Islam
CERT	Computer Emergency Response Team
CII	Critical Information Infrastructure
CISSP	Certified Information System Security Professional
CISA	Certified Information Systems Auditor
COE	Council of Europe
CRC	Convention on the Rights of Child
DDOS	Distributed Denial of Service
DNA	Deoxyribonucleic Acid
DNI	Dialed Number Identification
DNR	Dialed Number Recognition
DOS	Denial of Service
ECA	Electronic Crimes Act, (2007)
ECHR	European Convention for the Protection of Human Rights, (1950)
ECtHR	European Court of Human Rights
ECPA	Electronic Communications Privacy Act, (1986)
ETO	Electronic Transaction Ordinance, (2002)
EU	European Union

FBI	Federal Bureau of Investigation
FIA	Federal Investigation Agency
FIRST	Forums of Incident Response of Security Teams
G8	Group of Eight
GBPS	Gigabits Per Seconds
GCHQ	Government Communications Headquarters
GCSD	Georgian Center for Security and Development
GPS	Global Positioning System
HIPPA	Health Insurance Portability and Accountability Act, 1996
HQ	Headquarters
HRC	Human Rights Council
HRC	Human Rights Committee
IB	Intelligence Bureau
ICTs	Information Communication Technologies
ID	Identity Card
IoT	Internet of Things
ICCPR	International Covenant on Civil and Political Rights, (1966)
ICC	International Criminal Court
ICMF	International Conference on Magnetic Fluids
ICRMW	International Convention on Protection of the Rights of Migrant Workers and Members of Their Families (1990)
ILO	International Labor Office
IM	Interior Ministry

IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IRO	International Rights Organization
ISI	Inter-Services Intelligence
ISPs	Internet Service Providers
IT	Information Technology
ITU	International Telecommunication Union
ITU-D	International Telecommunication Union (Development Bureau)
IC3	Internet Crime Complaint Center
KP	Khyber Pakhtunkhwa
LEAs	Law Enforcement Agencies
MMS	Multimedia Messaging Services
MI	Military Intelligence
MIIT	Ministry of Industry and Information Technology
MOU	Memorandum of Understanding
MRTTR	Monitoring and Reconciliation of Telephony Traffic Regulations, 2010
NADRA	National Database and Registration Authority
NAP	National Action Plan
NR3C	National Response Center for CyberCrime
NSA	National Security Agency
NSN	Nokia Siemens Networks
NTC	National Telecommunication Corporation

NUST	National University on Science and Technology
NW3C	National white Collar Crime Center
OECD	Organization for Economic Cooperation and Development
OIC	Organization of Islamic Conference
PAK CERT	Pakistan Computer Emergency Response Team
PPC	Pakistan Penal Code, 1860
PBUH	Peace Be Upon Him
PECA	Prevention of Electronic Crimes Act, 2016
PC	Personal Computer
PGP	Pretty Good Privacy
PIE	Pakistan Internet Exchange
PISA	Pakistan Information Security Association
PTA	Pakistan Telecommunication Authority
PTCL	Pakistan Telecommunication Limited
RATs	Remote Administration Trojans
SAARC	South Asian Association for Regional Cooperation
SAC	Standardization Administration of China
SCO	Shanghai Cooperation Organization
SIM	Subscriber Identity Module
SMS	Short Message Service
SNIC	Smart National Identity Cards
STOA	Science and Technology Options Assessment
TCSTs	Tactical Communications Surveillance Technologies

TMS	Telephone Management Systems
TRIA	Telecommunications Regulatory Authority of India
UDHR	Universal Declaration of Human Rights, (1948)
UN	United Nations
UNODC	United Nations Office on Drugs and crime
UK	United Kingdom
UKUSA	United Kingdom - United States of America
USA	United States of America
VPNs	Virtual Private Networks

Table of Contents

Abstract

During the last few decades, the new methods of communication have been introduced into society because of technology. E-culture is getting more acceptance than the traditional modes of transactions. However, with numerous benefits that are associated with technologies there are also some embarrassments introduced by the same coin. Privacy of our digital information and data has become a dilemma. Our personal information and data have become more susceptible to be hacked and interfered. Such information and data require a great volume of security and safety. For this purpose, appropriate measures and expert skills are required. Pakistan lags behind to counter the privacy intrusions in digital sphere. It resulted into the threat of losing important information not only for citizens but also for national security of the Pakistan as well. Therefore, it is the need of hour to design an appropriate cyber privacy policy and security mechanism to protect and shelter the information and data of both, individuals and country on cyberspace. This research is aimed to analyse the right to privacy and threats which can seriously affect the citizen's essential information and data on cyberspace in Pakistan. In addition to it, this work examines the legislative measures of various developed nations and international organizations to protect the right to privacy of individuals. Finally, it is concluded with some recommendations to cyber security policy makers of Pakistan which can be adopted to prevent the cyberspace from unwanted intrusions.

Thesis Statement

Technology has changed the way, information is being received or sent, and, so it has affected the privacy rights of a person. Use of technology with internet together have provided many ways to keep an eye or to track a person without being noticed, resulting as a breach of privacy. This research will examine the growing privacy issues in cyberspace and a legal approach to defend and protect one's privacy rights in Pakistan.

Introduction and Scope of the Research

With the dawn of internet and technology, people have shifted to the cyber systems in their routine matters. All activities of human beings like business, defence, national security, health services, educational activities, entertainment and communications have implemented the new means of interaction. Technologies are used to make business more effective and efficient. Human services are improved with the help of technologies. As these technologies are proving reliable and adequate for individuals. They are shifting day by day to cyber systems and profiting themselves from these technologies along with online services, for example, arranging online meetings and placing internet for correspondences.[1] These online services have not only limited the costs but also saved the precious time of individuals. Moreover, the physical exertion and energy is also hoarded with the use of such technology.[2]

However, this technology revolution also brought some dangers and harms along with itself. It has opened a new avenue for crimes. Theft, invasion into privacy, pornography, hate

[1] Bakhsh, Muhammad, Amjad Mahmood, and Israr Iqbal Awan. "A comparative analysis of cybercrime and cyberlaws in Islamic Republic of Pakistan, Kingdom of Saudi Arabia, and the United Arab Emirates." *Imam Journal of Applied Sciences* 1, no. 1 (2016): 9.

[2] Kundi, Ghulam Muhammad, and Bahadar Shah. "eBusiness in Pakistan: opportunities and threats." *The Journal of Internet Banking and Commerce* 12, no. 3 (1970): 1-23.

speeches and other cybercrimes are the prominent features of this curse which is associated with digital revolution.[3] At present right to privacy has become a hot issue to address particularly, with reference to cyberspace technology as cyberspace is more vulnerable to cyber-attacks. For instance, withdrawal of money from Automated Teller Machine (ATM) can put one in the danger of many frauds like his bank account details and information of ATM cards can be copied to be used in future. Similarly, electronic and online means of filing taxes, refilling of prescriptions and internet-based services may be a source of electronic frauds of hacking and misuse of information. This high-profile nature of cyber-attacks are growing rapidly and speedily in our society. People have become acquainted with these dangers of technology either because of being a victim or knowing someone who has become the target of this increasing epidemic of crime. Now they want a crime free cyberspace where they can flow their information and data without any hesitation and fear. In this context, cybercrime has become a nightmare for the international community as well.[4] And to resolve the issues concerned many legislations have been enacted by different international communities. The following table sketches out some legislations in this regard.

IT Legislations in relation to privacy in cyberspace in Some Countries

Country	Year	Legislation	Contents
USA	1970	Freedom of Information Act	Permits individuals to access any information about themselves stored in the Federal Government Offices.
USA	1980	Privacy Protection Act	Provides protection of privacy in computerized and Other documents.

[3] Kundi, Ghulam Muhammad, Bahadar Shah, and Allah Nawaz. "Digital Pakistan: opportunities & challenges." *JISTEM-Journal of Information Systems and Technology Management* 5, no. 2 (2008): 365-390.

[4] Donn B. Parker, Fighting *Computer Crime: For Protecting Information*, John Wiley, USA, (1998): 10.

USA	1987	Computer Security Act	Requires security of information regarding Individuals.
USA	1997	Consumer Internet Privacy Protection Act	Requires prior written consent before a computer service can disclose subscriber's information.
USA	1997	Data Privacy Act	Limits the use of personally identifiable information and regulates "spamming".
Japan	2000	MITI Legislation for E-commerce	Legal Provisions for Electronic Signatures & Certification, and Foundation for Network-Based Social and Economic Activities
Canada	2000	Information Technology Act	Establish a legal framework for IT
Australia	2000	NSW Electronic Transactions Act	Application of legal requirements to electronic communications
UK	1998	Data Protection Act	Data protection and Right of data access
India	2008	Information Technology Amendment Act, 2008	It regulates the cyberspace in India and provides rules and regulations regarding different aspects of cyber law.
India	2013	The Privacy Protection Bill	To establish an effective regime to protect the privacy of all persons and their personal data

So far as concerned the issue of right to privacy and cyberspace laws in Pakistan, chapter II of the Constitution of Pakistan, 1973 deals with the fundamental rights. Article 9 of the Constitution of Pakistan, 1973 states that: "a person shall not be deprived of his life or liberty except in accordance with law". So, the provisions of this article are also closely linked with right to privacy. Further, Article 14 of the Constitution of Pakistan, 1973 explicitly deals with right to privacy. Article 14

(1) provides that: "the dignity of a man and the privacy of his home shall be inviolable save in accordance to law".

The concept of privacy is attached with the "dignity of a man". The "dignity of a man" is related to different aspects of dealings and routine affairs of life.

The National IT policy and Action Plan (2000) provides a brief recommendation for making cyber laws. It is mentioned in its articles to draft such laws which may be able to protect the privacy of individuals in cyber domain.

To provide a secure cyberspace and to make transactions safe, Pakistan has made efforts to legislate the effective legal framework. In this regard the Electronic Transaction Ordinance (ETO), 2002 is there to deal with business communications.[5] The objective of Act is to "recognize and facilitate documents, records, information, communications and transactions in electronic form, and to provide for the accreditation of certification service providers. With this legal framework we do have legal backing for electronic information and communication, as any written and signed document. With ETO in place, Pakistan has joined an exclusive band of countries that provide necessary framework and an impetus for growth of electronic commerce in Pakistan". In 2007[6] and further in 2009[7] two ordinances namely; the Prevention of Electronic Crimes Ordinance (PECO) were also adopted to address the cybercrimes but these laws lapsed due to not securing the parliamentary approval. After making several efforts to have an efficient code of cyber laws

---

[5] Electronic Transactions Ordinance, 2002.

[6] Prevention of Electronic Crimes Ordinance (PECO), 2007.

[7] Prevention of Electronic Crimes Ordinance (PECO), 2009.

the Prevention of Electronic Crimes Act (PECA), 2016 came into existence.[8] In this Act, a brief account is given to the various types of cybercrimes and punishments for such crimes are also provided in it.

The right to privacy is also provided in Holy Quran and Sunnah. Islamic teachings provide many provisions on right to privacy. Privacy is clearly guaranteed in Islam and it provides us an instrument to observe this right in our legal framework. The Holy Quran expressly talks about to the privacy of home.

By considering right to privacy in cyberspace is a hot issue to address, this research aims to analyse critically, cyberspace laws relating to right to privacy in the light of socio-legal context of Pakistani society.

The conceptual framework of the research is based on the question that to what extent the existing legislative framework in Pakistan is effective in protecting right to privacy in the cyberspace?

Hypothesis

This study is based on certain hypothesis like:

i. Cyber-crimes have put the rights of privacy of the people in danger and have made them concerned regarding their assets and transactions.

ii. Without proper legislation removing the cybercrimes is nearly impossible. It is frustrating when one cannot stop a cyber-attack and secure his personal information. Signing and ratifying the Cybercrime Convention should also be an early step at starting to secure cyberspace.

[8] The Prevention of Electronic Crimes Act (PECA), (2016) (Act No.XL of 2016).

iii. Legislation and implementation of data protection and privacy principles in a cyber-security policy can act as a proxy to reduce cyber threats, and cybercrime.

Research Questions

i. To what extent the existing legislative framework in Pakistan is effective in protecting right to privacy in the cyberspace?

ii. Do individuals in Pakistan have the right to privacy? Whether this right is guaranteed by the Constitution, International Treaties and/or by traditions and beliefs? What are the major challenges to right to privacy in cyberspace in Pakistan?

iii. Do individuals in Pakistan need specific legislation to protect their privacy in the ICT sector and what alternatives may be suitable for the Pakistani legal system to protect privacy in cyberspace?

Objectives of the Study

The objectives of the study are as follow:

i. To analysis the nature and concept of right to privacy in cyberspace;

ii. To find out the challenges related to privacy in cyberspace in Pakistan;

iii. To suggest legal remedies available to individual and public in the case of violation of right to privacy in cyberspace;

iv. To identify loopholes with regard to the cyberspace and data privacy in the existing legal framework of Pakistan; and

v. To achieve the same level of cybersecurity that is found in other developed countries.

Limitations of the Study

The study confines itself to examine the right to privacy with reference to cyberspace crimes from national and international perspective. Protection of right to privacy is investigated in the light of different national and international laws and human rights laws.

The empirical study has not been undertaken. The study is limited only to the critical analysis of cyberspace laws relating to right to privacy with reference to socio legal context of Pakistani society. The study has been confined only to the doctrinal research involving books, articles, International documents and relevant statutory material. Due to lack of literature in print form in this new area, the investigator has made extensive reference to the material available on the Internet.

Significance of the Research

This study begins in a three-part series on cyber security and right to privacy in cyberspace, focusing on how this issue affects our daily lives, our personal confidential information as well as our Nation and our National Security further it will help, how foreign hackers, who may even be sanctioned by their governments, make us dangerously vulnerable personally and as a Nation. This study is aimed to critically analyse the challenges which the government of Pakistan is facing while preventing the cyber-crimes in general and being a developing economy in particular. It also provides a way forward to deal with these cyber-crimes.

This study is important to make a demarcation that conventional security controls used before are outdated and are useless against the sophisticated and advanced malwares that utilize vulnerabilities, inside the digital world to capture the credentials of people and privileged users within it. It will be a significant step in analysing the recent attacks by indicating the sophisticated

capability of adversaries that have managed to penetrate even some of the most well protected networks by gaining deeper understanding of the core internal systems and processes with a lot of dedicated effort and collaborating with other adversaries to exchange information exploits working as an organized crime industry.

This study is an effort to bridge the gap between national and international laws relating to cyber security and data privacy to curb the cyber-attacks and to save the digital information. It will also inspire for further research in this field. On the basis of analysis, recommendations will be given for protection and promotion of cyberspace and data privacy under the auspicious of international and human rights law.

Research Methodology

The research will employ library-based data and internet facility for doctrinal research. Descriptive, analytical and critical methods of research have followed during this research. The relevant reports of different international monitoring organs as well as the reports of international bodies will be considered and examined. In line with the objectives of the dissertation, this work will present in order to build an argument on the relationship between cybercrime and data protection, both need to be conceptually unpacked and put in the context of a legal framework of reference. The corresponding part of this research is descriptive. These subjects are addressed in different sequences as the chapters progress, all of which sequences seem to naturally follow from the particular topics involved. This study presents the three dimensions of right to privacy in cyberspace. First, it means the technical and non-technical actions and measures which are adopted to protect computers, networks, software, data and other related digital technologies from all possible threats; Second, the level of protection and security because of adoption of such measures;

and Third, the true implementation of such actions and measures to protect data and information in digital sphere by making various policies.

Literature Review

In literature review of the study, analytical method will be followed to evaluate existing literature on the subject. This literature is related to establish a correlation between data protection rules and cybercrime prevention and cyber security from perspective of International Law, Human Rights Law (HRL), Islam and state law. The analysis of which necessitates examination and scrutiny of the legal framework regulating cybercrime cyber security and protection of data and privacy under International Law and HRL. Many scholars have thrown light on cyberspace, cyber security and right to privacy in digital world. A considerable work has been done in the perspective of digital age and the cyberspace. The researcher studied following material during her research:

Alisdair Gillespie, in his book, *Cybercrime: Key issues and debates*, discussed the cybercrime in a very comprehensive way. According to this book a cybercrime is also termed as computer crime. Cybercrime is categorized in three types. In first type of cybercrime, computers are targeted as a prey to damage it or to destroy the information and data installed in a computer or another network system. In this category computers are bulled by forwarding infected software, malware, viruses with the help of a computer as an armament. In second type of cybercrime, the computers are utilized as an armament. The traditional crimes are conducted with the help of advanced technologies and computers. Online frauds, pornography, cyber stalking and cyber spoofing are examples of such type of cybercrimes. In third type of cybercrimes, computers are used as a repository to collect and keep the information and data which have acquired by illegal means. However, this definition is not an international definition of cybercrime. It is also difficult

to design a such definition of cybercrime which may be accepted unanimously by international community. Though a crime may be denoted as a cybercrime which is committed on internet or some computer with the help of certain network and software in order to destroy another computer or to gain some information by illegal ways. Moreover, such cybercrime may be committed in any place of the world without territorial restrictions.[9]

Gillian Dempsey, Peter Grabosky, Russel G. Smith in thier book *Electronic Theft: Unlawful Acquisition in Cyberspace*, elaborated the effects of cybercrimes on national and international security. [10] They nicely analysed that in order to design a cyber security policy, it is necessary to involve the expert and skill persons.[11] It is further stressed that only an effective and efficient legal framework is sufficient to fight with cyber criminals. The authors argued that a cybercrime is committed only because of some technically expert person. Similarly, the defence against such attack can be made only with the help of certain skills and advanced techniques. This book is helpful in current research as it focuses on the need of an efficient and skilful mechanism to battel against cyber security and privacy intrusions.

Richard A. Clarke and Robert Knake in their book *Cyberwar: The Next Threat to National Security & What to Do About it*, elaborated certain cybercrimes in a very precise manner like web hacking, cracking of password, infringement of copy rights, stealing of data, child pornography etc.[12] which are directly related to privacy are discussed in this book. In some circumstances where

---

[9] Gillespie, Alisdair A. *Cybercrime: Key issues and debates*. Routledge, 2015.

[10] Dempsey, Gillian Grabosky, Peter and Smith, Russel G. *Electronic theft: Unlawful acquisition in cyberspace*. Cambridge University Press, Cambridge. 2001.

[11] Dempsey, Gillian Grabosky, Peter and Smith, Russel G. *Electronic theft: Unlawful acquisition in cyberspace*. Cambridge University Press, Cambridge. 2001.

[12] Richard A. Clarke and Robert Knake, *Cyberwar: The Next Threat to National Security & What to Do About It*. ECCO, 2010.

information or data is hacked or damaged or interfered in any way without lawful authority International forum is there to tackle this situation. International Criminal Court (ICC) is approached to deal with such criminal activities. However, in the absence of a uniform legal system, insufficient International legislation, deficient cooperation among international community along with inadequate domestic laws it is hardly possible to deal with the culprits of cybercrimes on international level. This book is of significant importance to be studied in order to know the nature of cybercrimes related to right to privacy in digital space. But this book does not unveil the situation of cybersecurity and right to privacy in Pakistan.

Donn B. Parker in his book, *Fighting Computer Crime: For Protecting Information*, analysed that the cybercrimes are more common to be committed with advanced manners.[13] Smart technologies and innovative methods are used to encroach the computers and Information Communication technologies (ICTs). To protect the data and information on digital devices it is necessary to improve the security of ICTs. The existing framework of cyber security is not reliable. If advanced measures of protection are not designed then there will be no place to keep the information and data secure from unlawful and unwanted intrusions. This is the need of the hour to adopt an appropriate IT security policy to combat the cybercrimes. It is the useful work for this research.

Mark.D. Rasch, in his book, "*Criminal law and the internet*", aptly explained that the online transactions have become a matter of routine in digital era.[14] Further, the use of internet and

[13] Donn B. Parker, *Fighting Computer Crime: For Protecting Information,* John Wiley, (1998).

[14] Rasch, Mark D. "Criminal law and the internet. in the internet and business: A Lawyer's guide to the emerging legal issues". *International Judicial Review*, 3(1). 1996.

computers have increased the danger of inference with privacy. Public and government both are equally at stake to become the target of cyber criminals. Moreover, the advanced and unconventional skills are used to hit a computer or network system to injure security of it and to obtain the required information. Most of the time the critical infrastructure system of a government is targeted. While in some instances the information of institutions or banks are stolen for financial advantages. In other cases, the corporations are attacked to make spying for some business gain. In order to control the cybercrimes on domestic and global level there is a need to adopt an appropriate legal measure. Developing nations are required to make cooperation with international community to implement advanced legal system and to eliminate the risks of cyber threats. However, this book does not explain the relation between cyber security and data privacy.

Marcos Christodonte II in his book *Cyber Within: A Security Awareness Story and Guide (Cyber Crime & Fraud Prevention)*, provided that in the growing digital world, Cyberattacks have become an everyday threat.[15] They not only affect financial and customer data, but machinery and industrial engineering companies through networked production systems and software-laden products. A holistic approach is needed to fully counter these threats. However, it does not discuss the legal approach towards cyber security and data privacy.

Christopher Hadnagy in his book, *unmasking the Social Engineer: The Human Element of Security*, discussed that the advanced technologies and computers are used to communicate with each other.[16] These communications may be made in business transactions or in the form of some

[15] Christodonte-II, Marcos. *Cyber Within: A Security Awareness Story and Guide.* (Cyber Crime &Fraud Prevention) proactive Assurance LLC. 2010.

[16] Christopher Hadnagy, *Unmasking the Social Engineer: The Human Element of Security,* Wiley; 1 edition. (2014).

personal or official affairs. The developing countries are also becoming familiar to use such ICTs and computer or internet to make interaction in business, commerce and government spheres. This dependency on certain networks and computers make the life easier and speedier. As the millions of miles are covered in the blink of an eye. But with all these comforts this blessing is disguised in a danger of cyber security. The information which is transmitted through this cyberspace and digital devices is remained in a great danger to be stolen or interfered by cyber criminals. However, this study does not provide any way out to combat the cyber security and privacy threats. Although it talks about the growing trends of digital communication in developing countries.

Lance James in his book *Phishing Exposed*, elaborated the siphoning off money through illegal cyber channels. However, it does not explain the cyber security measures in this regard.

Aub Chapman and Russell G. Smith, in their work *Controlling financial services frauds, Trends and Issues in Crime and Criminal Justice,* explained the nature of financial frauds with the help of technologies.[17] Further, certain way outs are also discussed to control the frauds in business sectors. Credit cards stealing and misuse of information is also addressed in this research. This research does not cover the situation of financial frauds with perspective of Pakistan.

Halder in his article, "Information technology act and cyber terrorism: A critical review", elaborated that the cyber criminals targeted the persons, institutions and certain business entities with the intention to harm their targets.[18] These offenders have a task in their minds to cause a damage to the individuals or organizations. Further, they also try to deprive their victims from

[17] A Chapman, and Russel G. Smith, "Controlling financial services frauds, Trends and Issues in Crime and Criminal Justice", 2: 189, *Australian Institute of Criminology,* Canberra, (2001).

[18] Halder, Debarati, Information Technology Act and Cyber Terrorism: A Critical Review (August 1, 2011). Available at SSRN: https://ssrn.com/abstract=1964261 or http://dx.doi.org/10.2139/ssrn.1964261

important and confidential information. Such type of cyber-attacks causes mental, financial and physical damage to the individuals. Sometimes the whole family suffer the pain in case of severe financial loss or some reputation harm. A person may be targeted to inflict a cybercrime either in a chat room or while using internet on his mobile or computer. Emails, Short Message Service (SMS), Multimedia Messaging Services (MMS) and like communications are also targeted. He critically examined the reasons behind the quick and speedy growth of cybercrimes.[19] He believes that the deficient in adequate cyber skills and knowledge are the main reasons of cybercrime in a society. He argues that with the development of digital age it is also the requirement of time to update the protective measures to make the proper use of technology. He further states that the licenced and authentic software shall be used so that the cyber-attacks may be prevented on initial stages. Trojans, viruses and pirated software are the most common reasons to damage the computer systems and information installed thein. This work is also beneficial for my research as it clearly talks about the preventive measures to secure the information and data in cyberspace.

Adam Salifu in his Article, "The impact of internet crime on development", Journal of Financial Crime", analysed that each day a large number of telecommunication correspondences are exchanged with each other.[20] Individuals use mobile phones and internet to send and receive message on electronic and digital space. According to a report "2 billion internet users and 5 billion mobile phone users are interacted daily in the world". Similarly, "294 billion emails and 5 billion SMS" are sent to each other. However, this interaction pays a price. As the reliance and confidence

[19] Halder, Debarati, Information Technology Act and Cyber Terrorism: A Critical Review (August 1, 2011). Available at SSRN: https://ssrn.com/abstract=1964261 or http://dx.doi.org/10.2139/ssrn.1964261

[20] Salifu, Adam. "The impact of internet crime on development". *Journal of Financial Crime*, Vol. 15. Number 4, 2008: 432-443(12).

on digital technology made human beings and institutions more prone to intentional damage by cyber criminals. Information and data are hacked or stolen from digital correspondences. With the advancement of technology, the crimes are also increasing rapidly. Internet frauds, financial damage, computer hacking, web jacking, email stalking malware attacks are the common types of cybercrimes. Cybercrimes are also a hindrance in economic and financial growth of a state. Although this research does not discuss the issues of cyber security and protection of data. It is limited only to the development and internet crimes.

Roderic Broadhurst and Lennon YC Chang in their article "Cybercrime in Asia: Trends and Challenges", argued that increase in the sale of personal computers has raised the threat of pirated software in markets.[21] Specially, the developing nations are found more involved in this business. China, Brazil, Malaysia, India and Pakistan are more prominent in this regard. In order to control the cybercrimes, the pirated software should be banned on domestic and international level. According to an estimate, China consumed about US$ 19 and India paid about US$ 2 billion on pirated and unlicensed software. This is also significant work as it directly discusses the situation of cybercrimes and cyber security in Pakistan. Moreover, it stressed to design such laws which may ban the pirated software from computer markets.

Ammar Yassir and Smitha Nayak in their article "Cybercrime: A threat to Network Security", discussed nicely the situation of cybercrimes in the globe.[22] They argued that the cybercrime is an equal evil for both nations – developed and developing. They further added that

---

[21] Broadhurst, Roderic, and Lennon YC Chang. "Cybercrime in Asia: trends and challenges." In *Handbook of Asian criminology*, pp. 49-63. Springer, New York, NY, 2013.

[22] Ammar Yassir and Smitha Nayak, "Cybercrime: A threat to Network Security", *International Journal of Computer Science and Network Security*, Vol.12 No.2. (2012).

countries shall make such legal system which may cater the existing situation of cyber security problem. Pakistan should also adopt an adequate cyber legislation so that the existing threats to cyber security may be handled properly. This work is also beneficial for the present study.

Ghulam Muhammad Kundi and Allah Nawaz in their article "Digital Revolution, Cyber-Crimes and Cyber Legislation: A Challenge to Governments in Developing Countries", analysed that the mobile phones and internet use is a vibrant threat to cyberspace in Pakistan.[23] They further added that cyber criminals adopt modern techniques and skills to commit a cybercrime. Business sectors and financial institutions are mostly targeted by criminals. In other cases, information is also stolen and misused. Sometimes cyber terrorism is also committed by using internet and various digital technologies.

Irfan Ghauri in his article "Electronic Crimes Act: Cybercrime to be made non-cognisable offence", discussed in this research that the cybercriminals hack the information from various institutions and websites.[24] Such confidential and sensitive information and data is sold in consideration of some price. A report revealed that the criminal's sale "the bank account details for US$ 10-125, credit cards information for US$ 30 and email account data or information for only US$12.85". This information may be about some sensitive matter but it has become a business for culprits to steal and sale the secret information. Further, the sold data is misused for causing damage to the subject. Financial, physical and mental harm is imposed to the victim. Moreover, to locate the source of cybercrime is also difficult. As information is stolen from one place and it can

[23] Ghulam Muhammad Kundi, Allah Nawaz and Robina Akhtar. "Digital Revolution, Cyber-Crimes And Cyber Legislation: A Challenge To Governments In Developing Countries", *Journal of Information Engineering and Applications*, ISSN 2225-0506, Vol.4, No.4, (2014).

[24] Irfan Ghauri, "Electronic Crimes Act: Cybercrime to be made non-cognisable offence", *The Express Tribune* with the International New York Times, (17 February, 2014).

be sold or misused from the other place. This situation has raised a challenge for government agencies to control the cybercrimes. It is a useful and valuable article for my research as it elaborated the cyber security challenges in detail.

Herhalt in his article, "Cyber-crime-A growing challenge for governments", argued that the cyber threats are used as a warfare instead of traditional weapons.[25] Political purposes are also diagnosed behind various cyber-attacks. It came into knowledge that in 2000 about 45 million computers were infected in the globe with a computer virus. A bug was transmitted through email around the world. Which resulted into the crack down a large number of computers and thus the whole system was disturbed. In other instances, political gain is achieved by hacking websites or by transferring false information. In another case a cyber-attack was made on Iran. In this attack a computer virus known as Stuxnet was as a weapon to explode and damage the Iran's Uranium nuclear plant. Cyber security is akin to the national security as well. This work will also help me in my research as it talks about the cyber security challenges for a government in a country.

Hackers also attacked the US Intelligence Agency and the German Federal Government. In these attacks the critical infrastructure system's information was collected and data was stolen. Spying was also made on various activities of government institutions. Similarly, in a survey of American Bar Association it was found that a law firm also faced the breach of data privacy. In another example the prominent law firm of New York also targeted by hackers for stealing of data. The north American Hospitals were also attacked by cybercriminals. In these attacks the viruses were transferred to the computer systems and records were damaged. In fact, the technology

[25] John Herhalt, "Cyber-crime-A growing challenge for governments", *KPMG Issues Monitor*, 8: 1-24, (2011).

advancement also gifted the mankind with cyber security threats. The ill minds use their efforts to attack a network for some financial gains.

Eduard Kovacs analysed in his report that Closed-Circuit Television (CCTV) cameras are attached with Internet of Things (IoT) botnet which is used to make Distributed Denial-of-Service (DDoS) attack.[26] This analysis was further followed with research. It was revealed that such technologies are also installed in home appliances and baby toys to keep their parents aware about the activities of their kids. Such type of things further exposed to be misused by criminals. Similarly, such techniques are also adopted to spy the individuals.

According to the report of the World Economic Forum's 2015 Global Risk cybercrime is one of the top ten risks to the economy of the world.[27] The developed countries are at more risks than developing nations. Such as US, Germany and China are at danger zones to become victim of advanced and smart cyber threats. According to the estimate of "Price Water House Coopers Information Security Breaches Survey, 2010" approximately 83% of owners of private businesses were made targeted and the amount of £27,000 - £55,000 was collected by cyber criminals. In Wales, £974m per year was reported to be lost in financial frauds, computer scams, information theft and data breach. The reasons behind such crimes are very common. The security systems are not updated. The computer literate persons are not hired to operate the sensitive and confidential information. Further, no adequate legal system is present to tackle such crimes. Similarly, there is

[26] Eduard Kovac; SecurityWeek.Com, http://www.securityweek.com/authors/eduard-kovacs (Last accessed: 21 November, 2018).

[27] Global Risks Report 2015. 10th Edition is published by the World Economic Forum within the framework of The Global Competitiveness and Benchmarking Network.

no harmony in national and international laws in order to make cooperation to deal with this borderless crime.

However, some efforts have been made by developed nations. The developing states also tried to follow the foot prints of developed countries in this regard but the nature of cybercrime is a great hurdle to control it. As first hurdle occurs in order to determine the origin of a cyber-attack. If in a case it is determined that from where it was originated the other barrier came into existence. Which make it difficult to determine the jurisdiction boundaries. The other obstacle is the deficiency of skills and expertness to detect or investigate a cybercrime. In some cases, because of this deficiency the critical information and data is not handled in secure ways. Just lack of proper security techniques in cyber domain results in great financial loss.

According to "Rob Wainwright who is the Director of Europol, Criminal Investigations of Cyber-Crimes", the cybercrimes are very difficult to be addressed. These crimes are sometimes not investigated only because of their borderless nature. The identification and tracking of a cybercrime is not an easy task. The developed nations are sometimes in better position to trace or control a cyber-crime as compared to the developing nations as these nations are not equipped with advanced technologies to locate a such sophisticated crime.

According to the Global e-Fraud Survey (2013) and KPMG Forensic and Litigation Services, it was reported that in order to handle a cybercrime in proper way, understanding nature of the threat is significant for consideration.[28] Further it is also required to know that how the online transactions and information on cyberspace may be made more protected. Further, the

[28] KPMG, *Global eFraud Survey*. KPMG Forensic and Litigation Services, (2013).

nature of some common cybercrimes in business sectors are also needed to be understand in order to prevent the damage. Most frequently reported crimes are "denial of service (DoS)", "distributed denial of service (DDoS)", advance fee fraud, cyber spoofing, cyber phishing, cyber stalking, cyber pornography, identity theft, web jacking, web hacking, information stealing, virus attacks, trojan attacks, spyware, malware and pirated software. However, these reports are limited only to the different kinds of cyber-attacks as no proper security measures are suggested to counter the cybercrimes.

This survey report revealed that developed nations are trying their best to cater the cybercrimes. They are also adopting proper laws to fight with this dangerous crime. with reference to Pakistan and other developing countries no such efforts are made to control the cybercrime on legal grounds. In Pakistan, cyber legislation is still in its infancy. While on the other hand, cybercrimes are happening more frequently in Pakistan especially in business domain and financial transactions. Further, the girls, children and women are also a prey of such cybercriminals. Cyber stalking and child pornography are frequently committed crimes in Pakistani society. The other cybercrimes are also common such as email stalking, email spoofing, online frauds, forgery of documents and stealing or misuse of information. However, because of lack of awareness and deficient of proper remedies many cases are not reported. In the year of 2013 only 16-20 cases were reported by women victims. Those were related to cyber stalking and information stealing. Pirated software is also used in Pakistan which results into the damage of the hard drives and weakening of protection measures. Similarly, unlicensed software is also sold in Pakistani computer markets. In order to prevent the cybercrimes, there must be proper legislation. Further enforcement mechanism must also be used to secure the cyberspace. With the development of

internet and technologies, public must also be aware to secure and protect their information on digital devices.

Yet there is lack of comprehensive research with reference to Pakistani socio-legal context. There is a need to improve and update the cyber laws with special reference to right to privacy and cyber security in cyberspace. Thus, a very limited research has been conducted in the context of a critical analysis of cyberspace Laws relating to right to privacy in the light of socio-legal context of Pakistani society. There is a need to do research in the perspective of right to privacy in cyberspace. Therefore, the researcher is going to analyse critically the existing cyberspace laws related to the right to privacy.

Scheme of Study

This study is based on the following scheme.

Chapter one is descriptive and specific to the concept and development of cyberspace technology. It defines Cyberspace Technology and evaluate history and development of Cyberspace Technology. It addresses those issues which arose due to Cyberspace Technology and discusses cybercrimes and threat to individuals and state's right to privacy.

Chapter two is specific to the development of the concept of right to privacy. It analyses international laws related to right to privacy. It defines the concept, philosophy, types and development of right to privacy. It analyses the provisions of HRL on right to privacy by focusing on relevant human rights instruments. It also discusses the regional HRL provisions and judicial opinions of the Courts. Further, it describes Islamic concept of right to privacy in detail. It also provides some examples where the Islamic law protects individual privacy. This linkage assists to

further develop a working definition of 'privacy' as the Islamic law is a major source of legislation for Pakistani law.

Third chapter describes the development of cyberspace legislation at international level by examining the laws of different countries, such as, USA, Europe and Asian countries. It also discusses the emergence of data protection in Cyberspace Technology by focusing on privacy regulations adopted by European Union, the UN guidelines on data privacy, 1990 and the Asia pacific economic cooperation (APEC), 2004. It discusses the role of UN Special Rapporteur on the right to privacy in cyberspace and the reports by the UN Rapporteur on the issue of cyberspace crimes while referring to regional mechanisms and the role of South Asian Association for Regional Cooperation (SAARC).

Fourth chapter focuses on the right to privacy and cyberspace laws in Pakistan. It examines development of Cyberspace Technology in Pakistan. This chapter analyses the laws relating to right to privacy in Pakistan, cyberspace laws of Pakistan and limitations on right to privacy in Pakistan. In line with previous chapters, the fifth chapter is specific to the critical analysis of cyberspace laws and right to privacy in Pakistan. It examines the cases of breach of right to privacy in Pakistani society. It also discusses victimized sectors of cybercrimes by focusing on Banking sectors, email, software piracy, social media, websites and internet. Further, it analyses critically the cyber legislation in Pakistan and highlight core cyber security issues of Pakistan. It highlights differences in the application of domestic and human rights safeguards. It also addresses the issue of non-harmonization of domestic laws with international law. It highlights the substantive and procedural aspects of challenges in state law with respect to cyberspace, cyber security and protection of data and privacy. Finally, conclusions are drawn and recommendations are given in

the end of study. The ultimate aim of this study is a try to provide an answer to the research question, and in particular to show the link between privacy and data protection, cyber-security, cybercrime and cyber legislation in order to protect the human rights of people in Pakistan.

Chapter One

The Concept and Development of Cyberspace Technology

Introduction

In the modern age, Cyberspace in general and Information and Communication Technologies (ICTs) in particular are the weapons which empower users worldwide to connect and associate with each other. Various activities are done by using cyber technology, such as, entertainments, business, education, awareness, marketing etc. However, there is need to ensure protection of data of users when they use it privately. As cyberspace is more vulnerable to cyber-attacks. The cyber criminals are highly skilled persons to interfere with the privacy of information and data. Such type of cyber-attacks restricts the performance of ICTs and hinder the services provided by internet and other communication networks. These malicious activities affect the ICTs related services in a very dangerous pattern. Certain limitations must be placed on users in order to avoid any fraud, disturbance with other's privacy, invasion on other's privacy rights, theft, pornography etc.[29]

In this context, this Chapter is divided into three Sections. Section one describes the definition of cyberspace. Section two discusses history and development of cyberspace technology. Section three addresses those issues which arose due to cyberspace technology and also talks about the cybercrimes. While discussing these issues it examines the threats to individual's right to privacy and state's security.

[29] David S. Alberts and Daniel S. Papp, *The Information Age: An Anthology on Its Impact and Consequences*, CCRP Publication Series, (1997): 16.

1.1 Definition of Cyberspace

Cyberspace means and includes all activities that have become dependent on technologies.[30] These technologies and network are running in a space known as cyberspace. In 1984, William Gibson used first time the term of "Cyberspace" in his Novel "Neuromancer". At that time, this term was used "to elaborate the entire networks of digital technology and all activities which take place or performed with the help of computer".[31] It is a transnational and transborder territory. In this place jurisdictional demarcations don't exist and people are free to interact "face to face without being face to face" on their computers and other devices. In present time this term "Cyberspace" is referred to a virtual world. It covers the whole range of computer and internet-based activities including the communications in the various fields like commerce, finance, health care, energy, entertainment, communications, and national defense. It is denoted to such actions which are done with the help of digital technologies and computer networks. Internet, computers and other modern ICTs are used to interact in cyberspace. This interaction is possible from thousands of miles away.

Cyberspace is paved on advanced semiconductors, advanced computers, fiber optics, cellular technology, satellite technology, advanced networking, improved human-computer interaction, digital transmission and digital compression. These technologies covered the gapes of communication and provided an advanced space -cyberspace- to human beings to be interacted world widely. In this space persons are connected with each other without traditional boundaries.

---

[30] Proceedings of a "Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Committee on Deterring Cyberattacks: Informing Strategies and Developing Options; National Research Council", (2010).

[31] Zahid Jamil, *Cyber Law*, Presented at the 50th anniversary celebrations of the Supreme Court of Pakistan International Judicial Conference on 11-14 August, (2006). Online available and retrieved from: http://jamilandjamil.com/wp-content uploads/2010/11/article_for_scp_50_anniv_v5.0.pdf, (Last accessed: 21 November, 2018).

These technologies not only eradicated the setbacks of primitive communication but also covered miles of distance on computer screens through networking on cyberspace. The whole world has become a global village and the interaction between persons is at the moment's notice in cyberspace.[32] This universal interrelated digital information and communications infrastructure is known as 'cyberspace' which supports almost every facet of modern society and provides critical backing to the economy, civil infrastructure, public safety, and national security.[33]

1.2 History and Development of Cyberspace Technology

The last few decades of twentieth century and the beginning of the twenty first century are labelled as the development of Information Age. This time frame is based on the revolution and proliferation of various information and communication technologies in human society and the capabilities of mankind to overcome the barriers resulted by such technology advancement. Advocates and supporters of the concept of Information Age argue that we have entered into a planet in which information and communications will become the dominant forces in defining and shaping human actions, interactions, activities and institutions.[34]

It has been proved from history that human beings ever remained needed to communicate and exchange information for various purposes such as to sound alarm, to give news, to provide information, to demand help, to formulate the sense of community and so on. However, this need faced complications in shape of distance, time or privacy. The instinct of privacy, security,

---

[32] David S. Alberts and Daniel S Papp, *The Information Age: An Anthology on Its Impact and Consequences*, CCRP Publication Series, (1997): 13.
[33] The White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure". (2009): iii.
[34] The White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure". (2009):14.

authenticity and timeliness forced mankind to develop communication technologies which resulted into birth of cyberspace.[35] To manage the hurdles of distance, privacy, time and security human beings adopted the methods of communication technologies in the form of drums, pigeons, torches, flags, flames, clay tabs, signals and signatures. All the primitive methods grew into modern technologies according to the needs and demands of humankind. From mid-nineteenth century to the mid-twentieth century, society has entered into a revolution of technologies in the form of telegraph, telephone, radio and television which minimized the constraints of time, location, privacy and security.[36]

By late 1980's the sun of modern technologies emerged in the form of great revolution and this time was pointed as "Information Age and Cyberspace" by analysts. Many technologies were introduced to mankind. Frances Cairn-cross in "The Death of Distance: How the Communications Revolution is Changing Our Lives, makes a bolder prediction" nicely argues that: "Think of the information revolution as one of the three great revolutions in the cost of transport. The nineteenth century, dominated by the steamship and the railway, saw a transformation in the cost of transporting goods; the twentieth century, with first the motor car and then the aeroplane, in the cost of transporting people. The new century will be dominated by the transformation in the cost of transporting knowledge and ideas in digital world". [37]

---

[35] Ibid at p15.
[36] Ibid at p15.
[37] Sandra C. Henderson Charles A. Snyder, "Personal information privacy: implications for MIS managers", *Information & Management*, 36(4): 213–220, (1999).

1.3 Issues Which Arose Due to Cyberspace Technology

Cyberspace is borderless and has no traditional form of jurisdiction. Usually, the affairs of cyberspace are easy prey to threats and dangers. Moreover, lack of skilled professionals and proper legislation make it more difficult task to keep this space free from criminals. As the cyber criminals are highly skilled persons to interfere with the privacy of information and data. Thus, the digital technologies generated safe havens for criminals to commit crime without being physically present in this spectrum.[38] According to Rob Wainwright, Director of Europol, cyberspace is a challenging task to investigate cyber criminals especially for developing world who is not expert in digital technologies. This complex situation is not mere a danger for national security but also to the financial health of a nation.

Due to its borderless nature, cybercrimes are more difficult "for governments and business to keep up with ever-changing technology and techniques used by cyber criminals".[39] Such type of cyber-attacks restricts the performance of ICTs and hinder the services provided by internet and other communication networks. These malicious activities affect the ICTs related services in a very dangerous pattern. Such intrusions impair the important affairs of government, institutions and individuals. For example, the stock exchange marketing, government websites, institutions facilities, mobile banking and money transfer services may be stopped as a result of hacking or hijacking of information and data. After such hacking the concerned information and data is used

[38] Carolyn Marvin, *When old technologies were new: Thinking about electric communication in the late nineteenth century*". Oxford University Press, *4(1)*: 88-97, (1988).

[39] Council of Europe, "Additional protocol to the convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems", (ETS 189), (2003).

for various criminal activities including the misuse of data, manipulation of information, exploitation of the owner or the other family members, breach of privacy and much more.

Sometimes, the individuals become the victim of privacy interference and lose their belongings including money and other properties. On the other hand, the institutions, organizations and government are also harmed by crashing the economics of country or controlling the stock exchange and financial affairs of monetary institutes. Fake figures and wrong information are entered to damage the stock share marketing. It is therefore the demand of the time that a well-defined and updated cyber privacy policy and security measures may be designed to defeat the attacks on information and to make the government, institutions, capital market services, and individuals safe and secure.

1.3.1 Cyber-Crimes in General

By the use of technology, various crimes can be committed especially cybercrimes. The nature of cybercrimes is borderless. For example, hacking an email account, wrong messages through digital devices for crashing aeroplane or boosting activities of terrorism etc.[40]

The main issue for the understanding of cybercrime is the absence of appropriate definition for the term of cybercrime, some jurists have tried to describe this word, but there is still no consensus on the definition of the word. The term "cyber-crime", is usually refers to all criminal activities which are done by using computers, Internet, cyberspace and the web all over the world". [41] In other words, it is a crime in which the computer is, either a target of crime or used as a tool to commit a

[40] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue and Julia Spiegel, "The Law of Cyber Attack". *California Law Review*, (2012).

[41] Andysah Putera Utama Siahaan and Muhammad Dharma Tuah Putra Nasution, "The Phenomenon of Cyber-Crime and Fraud Victimization in Online Shop," (2018).

crime. But this definition does not cover all aspects of cyber-crime, because sometimes even mobile phones are used for crime. Dr. Debarati Halder and Dr. Jayashankar has provided a useful definition. According to them, "cyber-crimes are intentionally committed crimes or criminal offenses against groups which deliberately damage reputations or cause physical or psychological harm to victims directly or indirectly by using modern telecommunication networks like internet or chat rooms, emails, notice boards, group chats, mobile phones, SMS or MMS". [42]

The term "cyber-crime" is used equally for technological offense, high technology crime, internet crime, economic offenses, electronic crime, digital crime, computers or others crime, which deals with the crimes that are done on computers.[43] It is better that instead of trying to understand cybercrime as a single incident, it may be better to see this term as a limitation of illegal activities, its 'common denominator' information and communication technology (ICT) has played a central role in their commission.[44]

Cybercrime is different from traditional crimes as in this category of crime criminals attack people "through network of hundreds of thousands if not millions of computers" and steal or destroy or damage critical infrastructure or hack important and sensitive information. Moreover, this nature of crime is different in various aspects. In some cases, computers are made targets to damage the hardware or software to destroy data or information. In other cases, computers are used as tools to send viruses, trojans and pirated software to steel or destruct data. In some situations, computers are dealt as accessories to save hacked data or information.[45] In all these

---

[42] *Encyclopedia of Cybercrime.*eds. Samuel C. and McQuade (Westport: Greenwood Press. 2009), s.v. "Cybercrime".
[43] Nappinai, N. (2010). Cyber Crime Law in India: Has Law Kept Pace with Emerging Trends? An Empirical Study. *International Journal of Commercial Law and Technology* , 22-28.
[44] MajidYar, *Cyber Crime and Society* (London: SAGE Publications Ltd, 2006), 9.
[45] Francois Mativat and Pierre Tremblay, "Counter-feiting credit cards", *The British Journal of Criminology*, 37(2): 165- 83, (1997).

circumstances computers are the tools to assist crimes or weapons to commit crimes. Cybercrimes are made possible with the help of computers in either way.[46]

Cyber-crime is a broader term. It involves each unauthorized activity performed in cyber domain to interrupt, steal, damage or alter any information or data. It may be committed against national security, economic security and individuals. It includes everything from electronic cracking to damaging critical infrastructure of a nation or to denial-of-service (DOS) attacks that cause electronic commerce sites to lose money. In this regard; Mr. Pavan Duggal, who is the President of www.cyberlaws.net; defined in a report the various categories and types of cybercrimes. According to him cybercrimes are of three categories. First category deals with cybercrimes against persons. Second category is related to the cybercrimes against property. The third category is labeled as Cybercrimes against government.[47]

The nature of cybercrime is radically different from other traditional crimes. It is also a great danger for international community to make the transactions safe and protected in cyberspace. As there is no border, no limit, no jurisdiction in this crime. It is an easy opportunity for criminals to commit it. Nations security are at stake because there is no international cooperation in this response. The rapid growth and use of ICTs have made the crimes more advanced. Cybercrime is an international crime which is rapidly growing day by day with the advancement of digital technologies. As more technologies are introducing more methods of committing crime are also flourishing. Criminals use these advanced technologies to danger the

---

[46] V. Karamchand Gandhi, "An Overview Study on Cyber crimes in Internet", *Journal of Information Engineering and Applications*, ISSN 2225-0506, Vol 2, No.1, (2012).

[47] Azeez Nureni Ayofe , "Approach To Solving Cybercrime And Cybersecurity", *International Journal of Computer Science and Information Security*, Vol. 3, No. 1, (2009).

mankind by adopting smart techniques and strong networks.[48] Research has revealed that "criminals are trading bank account information for US$10–125, credit card data for up to US$30 per card, and email account data for up to US$12.85".[49]

However, despite of the continuous growth of technology there is no response by international community to design even a single document to counter - this internationally agreed upon single definition - cybercrime.[50] Cybercrime is a common threat at international level for nations. There must be uniform international law to combat this crime. States, individuals and other groups are stake holders of such legislation. Many security concerns are involved in this danger. Criminals commit crimes without the fear of being identified by sitting thousands of miles away through internet. As international law is silent or provide such minor level of punishment as it has no deterrent impact on criminals. Another problem is the poor coordination and incompatibility of state laws with international laws although there is an international legal system in the shape of International Criminal Court (ICC) to punish such criminals.[51]

Cyber-world is a safe haven for cyber criminals. Many cyber experts suggest that appropriate cyber security techniques should be adopted to prevent criminal from accessing important information especially related to financial concerns. To control these crimes there is a need of experts like other forces to make a strong defense in cyberspace. Unlike other security concerns it demands only one expert individual not a proper army. According to Ronald Oble, the

---

[48] Donn B. Parker, *Fighting Computer Crime: For Protecting Information*. John Wiley, USA, (1998): 10.
[49] Irfan Ghauri, "Electronic Crimes Act: Cybercrime to be made non-cognisable offence", *The Express Tribune* with the International New York Times, (17 February, 2014).
[50] B Collin, *The future of cyber terrorism*, "Proceedings of 11th Annual International Symposium on Criminal Justice Issues", The University of Illinois at Chicago, Denning, D. E. (2001).
[51] Ghulam Muhammad Kundi, Allah Nawaz and Robina Akhtar, "Digital Revolution, Cyber-Crimes And Cyber Legislation: A Challenge To Governments In Developing Countries", *Journal of Information Engineering and Applications*, ISSN 2225-0506, Vol.4, No.4, (2014).

Head of Interpol, "an effective cyber-attack does not require an army; it needs just one individual. However, there is a severe shortage of skills and expertise to fight this type of crime; not only at Interpol, but in law enforcement everywhere".[52] Skilled persons, expertise and e forensic techniques may make it possible to secure cyber-world from hackers, viruses, malware and trojans. Most of the installed software are pirated which are open invitation for criminals to commit cybercrimes.[53]

1.3.2 Threat to Individuals' Right to Privacy

With the innovation of technologies, the manner to ensure or to infringe the privacy has been changed. Some innovations like printing press and internet, had expended the capacity to share data and information as well as introduced new methods to violate the privacy. [54] Advancement in technology has made it easy to collect sensitive information and data.

The expended flow of communication technologies along with its ability to accumulate, investigate and transfer data had made people to demand the enactments dealing with data and information privacy. Computer networks connected with fast internet systems and advanced processing techniques can make extensive record of any individual without any single central computer framework. Development in technology and communication introduced by the defense industry had made law enforcement bodies, civilian organizations and privately-owned businesses more concerned about their privacy. As indicated by surveys, privacy infringement has become a big issue in present time before any other time in history.[55] Unanimously, people of various

---

[52] Peter N. Grabosky and Russel G. Smith, *Crime in the digital Age: Controlling telecommunications and cyberspace illegalities*, Federation Press, Sydney/Transaction publishers, New Brunswick, (1998).
[53] John Herhalt, "Cyber-crime-A growing challenge for governments", *KPMG Issues Monitor*. 8: 1-24, (2011).
[54] Samuel Warren and Louis Brandeis. "The Right to Privacy", *Harvard L.R.* 193 (1890).
[55] Simon Davies "Re-engineering the right to privacy: how privacy has been transformed from a right to a commodity", in Agre and Rotenberg, "Technology and Privacy: the new landscape", MIT Press, (1997): 143.

countries have demanded to make privacy laws and to secure their data and information from every type of interference. Human rights activists assert that developing countries are more vulnerable to breach of privacy as they have insufficient securities to preserve information. At present, there is obstruction to the trade in communication technologies.

The ability and limit of sharing information is rushing quickly because of developed techniques. It resulted into the privacy encroachment and the risk to interfere with data and information has been raised consequently. A large number of these innovations were embraced and realized without legitimate assurances, for example, Identity frameworks.

The prominent technologies of privacy invasion are discussed below.

1.3.2.1 Identity (ID) Cards:

ID cards are used for a number of purposes. Race, political associations and religious beliefs were usually at the core of old ID structures. The danger of religious segregation, political radicalism and insurgency are the foundation of ID frameworks which would compel foes of the State to be registered and in this way, they are prone to be exposed.

In Pakistan, these cards are also utilized to implement a quota system along with other purposes. Recently ID cards are connected to national registration system which is related to the basic government administration. In this way ID cards turned out to be more noticeable part of a big system. In Pakistan, Spain, Portugal, Thailand and Singapore ID cards are directly connected to government administration. Microchip innovation and magnetic stripes have made ID cards a source to approach various government services. In this way ID cards are turned into a combination for demanding government services and a proof of identification. This idea of innovation has also

enhanced police powers. Even in law abiding countries, police hold the privilege to request ID card on fear of detainment.[56]

In various nations, these frameworks have been criticized on privacy interests. In 1998, the Philippine Supreme Court held that national ID card system infringes the fundamental right to privacy.[57] In 1991, the Hungarian Constitutional Court decided that a law allowing a multi-purpose with this identification disregards the protected right to privacy.[58]

1.3.2.2 Biometrics:

Biometrics technology is related to the gathering, handling and keeping the data of a person's physical attributes for the purpose of identification and proof. The most well-known types of biometric ID are retina scans, hand geometry, thumb impression, fingerprints, voice acknowledgment, and digitized photos. This innovation has grabbed the attention of governments and organizations on the basis of difference from other sources of identification. Unlike ID cards or papers, it has the ability to precisely and personally recognize the subject.[59]

The most questionable type of biometrics is Deoxyribonucleic Acid (DNA) distinguishing proof. It is famous from new examining innovation as it can consequently held DNA tests against

---

[56] Kundi, Ghulam Muhammad, Allah Nawaz, Robina Akhtar, and I. E. R. MPhil Student. "Digital revolution, cyber-crimes and cyber legislation: A challenge to governments in developing countries." *Journal of Information Engineering and Applications* 4, no. 4 (2014): 61-71.

[57] *Ople v. Torres, G.R. 127685, July 23, 1998* (Philippine Supreme Court Decision about the National ID System). http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Identity.html (Last accessed: 20 November, 2018).

[58] Constitutional Court Decision No. 15-AB of 13 April 1991, http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Identity.html (Last accessed: 20 November, 2018).

[59] P De Hert & S Gutwirth 'Data protection in the case law of Strasbourg and Luxemburg: Constitutionalization in action' in S Gutwirth *et al. Reinventing data protection?* (2009): 3.

an extensive database in a short time. In the US, Germany and Canada police department are making national databases of DNA. In the UK and the US, police have been requesting that all people in a specific territory should provide intentionally test samples or face investigation as a suspect.[60]

1.3.2.3 Surveillance of Communications:

Almost all nations have been imposed some type of wiretapping capacity over phone, fax and message correspondences.[61] By and large, these steps have been approved by law enforcement offices. Illegal Wiretapping have been reported in many nations.[62] It happened on a large scale including a huge number of illicit taps. This misuse may affect anybody. The main prey of this danger are political persons, students' leaders, union leaders and human rights activists. The US has made efforts to confine individual's privacy and upgrade the ability of its police forces and intelligence services to spy phone calls of its citizens. This battle had adopted two legitimate techniques. The first made it required for all advanced phone switches, cell and satellite telephones and all communication technologies to install surveillance innovations. The second observed to restrict the encryption programming that gives encryption techniques, a procedure which enables individuals to secure their communications and documents and keep others away from perusing them.[63] Encryption is the secured way to protect data and information of individuals. Encryption has turned into the most vital device for insurance against surveillance. A message is twisted only for the purpose that the proposed beneficiary may have the capacity to unscramble it and may be

---

[60] Rick Howard, *Cyber Fraud Tactics, Techniques, and Procedures*. New York: Auerbach Publications, (2009).
[61] Ananda Mitra, *Digital Communications: From E-mail to the Cyber Community*, New York: Chelsea House, (2010).
[62] Gutwirth, Serge, Ronald Leenes, Paul De Hert, and Yves Poullet, eds. *European data protection: coming of age*. Springer Science & Business Media, 2012: 6.
[63] Banisar and Davies, *The Code War*, Index on Censorship, ISSN: 0306-4220 Online ISSN: 1746-6067, sage publications. Volume 27 Issue 1, January (1998): 162–168.

able to get the message hidden within it. The "Pretty Good Privacy" (PGP) is the well-known encryption program and has more than 100,000 clients, including human rights activists, for example, Amnesty international.

1.3.2.4 Internet and Email Interception:[64]

In most countries in the world the law enforcement institutions and security providing organizations had quickly shifted to control and break down email and other internet-based movements.[65] In UK, law enforcing institutions have demanded the control over email activity. They claimed that people's movements on internet ought to be admissible through understandings between police and internet Service Providers (ISPs). This move caused alert for rights of people requesting that email capture should also be protected and prevented in the manner of the phone capture.[66]

In Singapore, ISPs are managed by government-controlled or related associations and in this way transfers data to government offices regularly. In Russia, a suggestion is under consideration that all ISPs should put a black box and rapid connection linked to the Federal Security Service so that, the "Anonymous remailers", may stop data assessment. In Information Technology Act, 2008 India declared its Critical Information Infrastructure (CII) as the computer resource; the destruction of which, shall have a debilitating impact on national security, economy,

---

[64] "intercept", in relation to a communication, means listening to, monitoring, viewing, reading or recording, by any means, such a communication in its passage over a tele- communications network without the knowledge of the person making or receiving the communication.

[65] Ibrahim Baggili, *Digital Forensics and Cyber Crime*. New York: Springer, (2011).

[66] P. M. Schwartz and D.J. Solove, "Reconciling personal information in the United States and European Union", 102 *California Law Review*. (2014): 879.

public health or safety.[67] They may shred identification of data from messages and emails. They are equal to Post Office (PO) Box addresses. Additionally, they are restricted from police and intelligence administrations. In Pakistan, the Internet Service Providers (ISPs) are also directed to control and retain the traffic of internet data under Prevention of Electronic Crimes Act (PECA), 2016. Further, PECA (2016) demands from ISPs to maintain the collection of real time in order to track the activities of internet users.[68]

In Finland, a mainstream anonymous remailer has been closed because of legitimate difficulties that compelled the administrator to uncover the name of one of the clients. The retaining of data regarding particular Internet visits has turned out to be one of the greatest developing dangers to Internet protection. Each time a client gets to a website page, the server records the page logs of the client's Internet address alongside the time and date. Few sites put "cookies" on a client's machine to track individuals' activities in detail.

Some websites request for the client's name, address and other personal detail of an individual to permit the access. Web based shopping are correspondingly recorded. On-line stores give great value to such data and sale it to other service providers, advertisers and different associations. Some specialized arrangements have been conceived to counter such practices. "Anonymising" programming enables clients to peruse the Web without sharing their Internet address. "Cookie cutter" programs hinder the websites to spread cookies on client's computer. These programs are installed into the manufacturing of systems. Anonymous digital cash gives

---

[67] Diamond, Jonathan. "Guidelines for the Protection of National Critical Information Infrastructure: How Much Regulation?" 31 July. (2013). [Online]. Available: https://cisindia.org/internet-governance/blog/guidelines-for-protection-of-national-criticalinformation-infrastructure.

[68] Haroon Baloch. "Internet Rights and Legislation in Pakistan: A Critique on Cyber Crime Bill 2016". http://www. netfreedom. pk/ wp- content/ uploads/2016/06/CSO- criticism- on- PECB-2016_IssuePaper (Last accessed: 16 November, 2018).

purchasers a chance to make payments without uncovering their personality. These methods are often used to secure the information and data on internet tracks.[69]

1.3.2.5 Video Surveillance

Recently, the utilization of Closed-Circuit Television (CCTV) Cameras across the globe has developed to a remarkable level. It is estimated that 150 to 300 million pounds are spent annually on surveillance industry including approximately 200,000 cameras observing only public areas.[70] Number of towns and urban communities are adopting CCTV monitoring of public territories, lodging homes, auto parks and public offices. It is assessed that the use of this technology is raising 10 to 15 percent yearly. In Britain numerous Central Business Districts are observed by camera frameworks equipped with the facilities of zoom electromagnet abilities. Their utilization for the security and observance of private property is also getting prevalent.[71]

These camera networks are equipped with advanced innovation. The characteristics of night vision, computer-based activity, and movement identification are incorporated in these cameras. Which enable the administrator to direct the system to issue red alert when anything appears unusual. To ensure the security of cameras from any damage bullet proof covering and self-protection systems are introduced. The clearness of the photos is normally superb in these cameras as many of them are capable to pursue cigarette parcel hundred meters away. These cameras can frequently work in pitch obscurity and anonymity by making pictures as clear as

---

[69] O Lynskey, "Deconstructing data protection: The 'added value' of a right to data protection in the EU legal order", 63(3) *International and Comparative Law Quarterly*, (2014): 569.

[70] House of Lords, "Science and Technology Committee", Fifth report, "Digital images as evidence", 3 February, (1998).

[71] Stepehen Graham, John Brooks, and Dan Heery, "Towns on the Television: Closed Circuit TV in British Towns and Cities", Centre for Urban Technology, University of Newcastle upon Tyne, (1995).

visible in day time. The innovation is eventually combined with modern software programs that are able to identify the faces, environment analyses of a group, and examining of the zone between skin surface and garments. The power and abilities of these cameras are constantly increasing, while the cost and size are diminishing. It is sensible to expect that secret visual observation will be a universal issue in a few decades.[72]

The CCTV technology is not limited to the Britain only.[73] Sweden is also considering to relax its privacy laws and to allow CCTV cameras to observe public places.[74] While Norway has incorporated particular provision of such observation in the data protection laws act. CCTV usage has been developed unprecedently in North America and Australia to monitor public territories. In Singapore, they are generally utilized for traffic administration and to control collusions.[75]

It is the opinion of some viewers that the societies are going towards a drastic change. The innovation and advancement of technology has been portrayed as the "fifth utility." CCTV is being introduced into the urban communities similarly in the manner of the power supply and the phone systems. CCTV is significantly changing the condition of urban areas and presently working as a critical piece of the central administration of these areas. Visual surveillance is turning into basic elements of municipal communities and it is installed in houses, business places and traffic areas. CCTV pictures may be seen as only sort of important information and will be considered as a

---

[72] AOA Yusuff, "Legal issues and challenges in the use of security (CCTV) cameras in public places: Lessons from Canada", 23 *Sri Lanka Journal of International Law,* (2011): 33.

[73] Stepehen Graham, John Brooks, and Dan Heery, "Towns on the Television: Closed Circuit TV in British Towns and Cities", Centre for Urban Technology, University of Newcastle upon Tyne, (1995).

[74] Ibid at p10.

[75] Report of Electronic Privacy Information Centers, "Privacy and Human Rights 2006–An International Survey of Privacy Laws and Developments" (EPIC 2006), http. www epic org. (Last accessed: 16 November, 2018).

worth added item. In Pakistan, CCTV cameras are also installed at Lahore and Islamabad in the name of safe city project.

1.3.2.6 Workplace Surveillance:

Workers, in almost every nation; are powerless against the far-reaching surveillance by their employers. Legal insurances are useless and careless in such conditions as in most of the situations it is the basic requirement of the employers. In many countries, bosses can tap telephones, view email and watch PC screens of their employees. Employers can follow their discussions, break down their PC security codes, monitor them by CCTV cameras and observe their activities by tracking devices. Even in some situation, urine is examined to recognize drugs utilize, and may be ordered for the announcement of personal information.[76]

Powerful devices and techniques are utilized to observe the employees. These technologies can monitor the "keystrokes" to decide whether the employer has effectively used his time even during his phone calls discussions. This procedure is known as "performance monitoring" by software organizations. In working environments operated by skilled professionals, the employers demand to keep an eye on every movement of his employee`s activity. New network systems connected with PCs are developed with the opportunity to figure out which programming is being run, how frequently, and in what way. An exhaustive review track provides a complete profile of every client and a scene of how the employees are working with their machines. The focal control over every individual's PC is given to the employer. An administrator can alter or suspend programs on any machine from a remote distance. These innovations affect each part of a laborer's

[76] Yusuff, Abdulwasiu Ojo Akorede. "Legal Issues and Challenges in the Use of Security (CCTV) Cameras in Public Places: Lessons from Canada." *Sri Lanka J. Int'l L.* 23 (2011): 33.

life. Smart cameras' screen monitors the conduct of a worker. Like the ID identifications which track a worker's activities around a building, the Telephone Management Systems (TMS) observes the phone utilization and the place of call. Numerous tests such as psychological assessment, general intelligence tests, inclination tests, execution tests, professional intrigue tests, identity tests and honesty tests for the most part of time are evaluated electronically. Observation and checking have become prominent segments of current data frameworks.[77]

However, organizations declare that all observation is legitimate, but it is observed that all practices of checking are not lawful. For instance, one US manager introduced cameras to visualize every individual on workstation. Despite of the fact that administration guaranteed that the technology was being installed exclusively for security and safety measures anyhow, two workers of station were suspended for leaving their workstations for visiting toilet without authorization. As per a report, 1993 of the International Labor Office, the exercises of association agents on the floor were additionally represented as "chilling impact" on specialists who knew their discussions were being checked. A trend of such instances of misuse of visual observation and tracking has provoked security and privacy measures in the working environment. In a survey conducted in 1991 in the US, it was held that 62 percent of workers criticized and contradicted with visual surveillance. 38 percent of workers were totally against of such type of monitoring. American Management Association (AMA), exposed that two third of American supervisors keep an eye on their laborers through email and telephone calls tracking.[78]

---

[77] Report of Electronic Privacy Information Center's, "Privacy and Human Rights 2006–An International Survey of Privacy Laws and Developments" (EPIC 2006), http://www.epic.org. (Last accessed: 16 November, 2018).

[78] Report on Electronic Monitoring & Surveillance, American Management Association, (1997), Online available at: <http://www.amanet.org/survey/elec97.htm> (Last accessed: 20 November, 2018).

In a report published in the name of Job Stress: The 20th Century Disease, the ILO points towards growing evidence of problems around the world, including developing countries, where companies are doing little to help employees to cope with the strain of modern industrialization. The report also revealed that as the use of computers which has been spreaded throughout the world, workers in many countries are being subjected to new pressures, including electronic spying by bosses.

A survey conducted in 1990 by broadcast communications laborers partially supported by the Communications Workers of America (CWA) told that 84 percent of observed representatives have high pressure of stress rather than 67 percent of unmonitored workers. Another report by the US Office of Technology Assessment, additionally found that work environment observance adds pressure and causes stress-related ailment.[79]

In Britain and the US, there are couple of lawful limitations on video observation unlike to the laws of Austria, Germany, Norway and Sweden in which administration is required to enter into agreements with employees. This circumstance has been analysed in the European Court of Human rights (ECtHR). A British Assistant Chief Constable Allison Halford objected against police that because of her sex segregation her office telephone had been disturbed. While the British government affirmed that this was an altogether legitimate and appropriate step but Halford kept it up and claimed that her right to privacy had been interfered, mentioned in the European Convention on Human Rights (ECHR). The court decided that the police exercised unlawful authority by tapping Ms Halford's telephone.[80] This manner appears likely the breach of privacy

[79] Report of the office of Technology Assessment, New Technology, New Tensions, September (1987).
[80] *Halford v United Kingdom*, (Application No 20605/92), 24 EHRR 523, 25 June, (1997).

laws embodied in European Telecommunications Directive (ETD). It further stated that it has become norm that the employers' calls shall be monitored by their bosses which is illegal.

West takes the liberal and innovative steps to regulate and monitor the surveillance, wiretapping, individual's ID frameworks, data mining, encryption control and much more.[81] These practices and the largescale developments mentioned above, had also influenced the developing nations to conduct the surveillance and observation. Developing countries depend upon the first world nations to receive innovations of technologies, for example, computerized wiretapping devices, interpreting gear, scanners, bugs, following and tracking devices and computer frameworks. This exchange of innovation from first to third world is presently a profitable hobby for the arms business.[82]

As per a 1997 report "Assessing the Technologies of Political Control" conducted by the European Parliament's Civil Liberties Committee and European Commission's Science and Technology Options Assessment office (STOA),[83] these advanced technologies are mostly used to track and follow human rights activists, writers, leaders, minorities, students, dissidents, union leaders and political adversaries. The report asserted that such advancement can apply a great 'chill impact' on the individuals who may wish to take a contradicting perspective and others may seek legal remedies to meet these challenges.

A great number of ID frameworks are likewise valuable for checking major portion of populous. "Privacy International" found that without significant legitimate or sacred assurances

---

[81] Simon Davies and Ian Hosein, "Liberty on the Line" in Liberating Cyberspace, Pluto Press, London, (1998).
[82] Banisar, David, and Simon Davies. "Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments." *J. Marshall J. Computer & Info. L.* 18 (1999): 1.
[83] Published by "Science and Technology Options Assessment (STOA)", Ref: project no. IV/STOA/RSCH/LP/politicon, p1

is a continuing struggle to define it clearly and in such a way as to allow the definition to evolve along with digital technology. The ITU developed a paper offering a common definition of cybersecurity for the World Summit on the Information Society in 2005.[86]

The former US Director of National Intelligence, retired Admiral Dennis Blair, testified in early 2010 that increasingly sophisticated enemies "severely" threatend the US information systems: "Sensitive information is stolen daily from both government and private sector networks, undermining confidence in our information systems, and in the very information these systems were intended to convey. Malicious cyber activity is occurring on an unprecedented scale with extraordinary sophistication.[87]

Like other security concerns cybersecurity is also related to the protection, confidentiality, integrity and safety from destruction, interference, damage and misuse of information in digital technologies. Cybersecurity involves the protection of both types, passive and active security. When it relates to passive security measures it means the adoption of various measures to stop the criminal attacks. Passive defense techniques are designed in system itself which makes the attacks difficult and protect it from damaging. It also includes the criminalization of certain acts in cyberspace by making laws and policies. Passive defense techniques are actually precautionary measures that are invited to hinder the access of crimes by early warning system and policy making for cybercrimes. On the other hand, active cyber security relates to the actual tracking and stopping of cyber-attack or to prevent the attacker from making other episodes. Passive security is far better

[86] ITU, A Comparative Analysis of Cybersecurity Initiatives Worldwide, in WSIS Thematic Meeting on Cybersecurity, (2005).

[87] Blair, Dennis C. *Annual threat assessment of the intelligence community for the Senate Select Committee on Intelligence*. OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE WASHINGTON DC, 2009.

technique from active defense as it is more difficult to chase the attacker in a boundaryless digital world as compared to prevent him from committing attacks.[88]

Why Cyber Security is Necessary for State's Security?

The value of cybersecurity depends upon its need. If people are dependent on digital technologies then obviously, they have a dire need to protect them and making of appropriate policies. But if they don't have such technologies then adoption or making of these policies will be only a wastage of time and minds. Another important notion of cybersecurity is that how much it is important for them. Do they involve digital technologies to handle our critical infrastructure? Or our national security is dependent on it? It includes military application of computers and other telecommunications, protection of intelligence data and information. This definition of national security relates to the cybersecurity only in one situation if the nation is dependent upon digital technologies for the protection of critical infrastructure.

For some nations, cybersecurity is national security as it deals with their defense policies and military's operations of digital technologies. For others, it may not be important as a national concern but only as an economic concern because of business dependency on such technologies. While for other nations, it may be important only in the manners of governance or cooperation with other nations or only to provide basic necessities of education or health care. In this way, cybersecurity concern is a fashion of security branches hence these branches are sure to provide

[88] Cole, Kristina, Marshini Chetty, Christopher LaRosa, Frank Rietta, Danika K. Schmitt, Seymour E. Goodman, and G. A. Atlanta. "Cybersecurity in africa: An assessment." *Atlanta, Georgia, Sam Nunn School of International Affairs, Georgia Institute of Technology* (2008): 7-8.

security from interruption or destruction. It is the responsibility of institutions to adopt security measures according to the need, demand and value of matter. [89]

Cyber insecurity is a situation which can stem from the flaws or weaknesses in a system's hardware or software program. It can be the result of states, individuals or other groups' conduct who deal with it. Cyber insecurity appears in the form of cyber warfare, cyber-attacks on critical infrastructure, scams, fraud, destruction of sensitive information and much more. It is a great threat to a nation as it is transborder and transnational.[90] President Obama's 2009 Cyberspace Policy Review concludes: "a growing array of state and non-state actors such as terrorists and international criminal groups are targeting U.S. citizens, commerce, critical infrastructure, and government. These actors have the ability to compromise, steal, change, or completely destroy information".[91]

In 1947, after the advent of world War II, the legislatures of the US, the UK, Canada, Australia and New Zealand adopted a National Security settlement known as the "Quadripartite," or "United Kingdom - United States" (UKUSA) agreement. Its aim was to sign a bond in which a common National Security objective may be attained. According to the understanding, the five countries divided the earth into five domains, and every nation was allocated specific targets. The UKUSA pact established phrasing, code words, care of techniques, plans for collaboration, sharing of data and access to services. One essential segment of the agreement was the trading of

---

[89] Cole, Kristina, Marshini Chetty, Christopher LaRosa, Frank Rietta, Danika K. Schmitt, Seymour E. Goodman, and G. A. Atlanta. "Cybersecurity in africa: An assessment." *Atlanta, Georgia. Sam Nunn School of International Affairs. Georgia Institute of Technology* (2008): 9-10.

[90] A recent example is the comprehensive and influential "Securing Cyberspace for the 44th Presidency," A Report of the CSIS Commission on Cybersecurity for the 44th Presidency, (2008).

[91] House, White, and Comprehensive National Cybersecurity Initiative. "Cyberspace policy review." *Assuring a Trusted and Resilient Information and Communications Infrastructure." Washington, DC: White House* (2009).

information and employees. The bond infers that agents from the New Zealand signals intelligence agency Georgian center for security and development (GCSD) would be able to work from the Canberra offices of Australia's Defense Signals Directorate[92]to catch domestic correspondence and data and forward it to the Australian intelligence offices without prior permission of either country.[93]

The most powerful union inside the UKUSA relationship is between the US National Security Agency (NSA) and Britain's Government Communications Headquarters (GCHQ). The most authoritative office in the union is Menwith Hill, in the north of England. With an attractive computer working services, the base has the ability to spy quietly on wide range of communications. With the formation of Intelsat's network and advanced broadcast communications, Menwith and different stations have built the capacity to spy on a broad scale of fax, wire and voice messages. It is broadly trusted that Menwith Hill has around 40,000 lines associated with it, through which access could be made to a lot of European and Soviet correspondences.

European Parliament issued a report in 1997. It is asserted in this report that "project Echelon" enables the NSA to look almost all information communications for "key words". Messages from this information are not investigated on daily basis, nor the filtering is done continuously, however day by day reports give "precursor" information which supports intelligence offices to achieve targets. Programmed checking of voice is not far away. A voice

---

[92] Bamford, James. *The Puzzle Palace: a report on NSA, America's most secret agency*. Houghton Mifflin Harcourt, 2018.

[93] Richelson, Jeffrey T., and Desmond Ball. *The ties that bind: Intelligence cooperation between the UKUSA countries, the United Kingdom, the United States of America, Canada, Australia, and New Zealand*. St Leonards: Allen & Unwin, 1985.

acknowledgment framework called "oratory" has been utilized for a few years to catch and break down telephone calls of diplomatic agents.[94] The report "Assessing the Technologies of Political Control states inside Europe" says that all email, phone and fax correspondences are routinely spied by the US's NSA exchanging all material data from the European territory through the key center of London at that point by satellite to Fort Meade in Maryland by means of the urgent center point at Menwith Hill in the North York fields in the UK. The report generated a threat in Europe which on September 14, 1998, drove a discussion in the European Parliament. A "compromise resolution" confined that day by the four noteworthy parties called for more prominent responsibility and "defensive measures" over the exercises of security offices. In this way it is important to build such security measures which can protect a state from illegal and unauthorized interference into its cybersecurity and privacy.

Conclusion

From the above discussion it is concluded that the ICTs have evolved the cyberspace to assist a growing portion of the work force devoted to the generation, transmission, storage, processing, retrieval, and general use of information. However, the wide range of innovations caused various unwanted impacts including threat to privacy on human lives. Technology development and the dawn of cyberspace made it a challenge for individuals to keep their information and data secure. The situation of cyber security is more alarming and scarier in developing countries. With the advancement of technology, it is also important to upgrade the legal framework to secure the

[94] "European Parliament, Scientific and Technological Options Assessment (STOA), An Appraisal of Technologies of Political Control", 6 January, (1998), Online available at: http://jya.com/stoa-atpc.htm (Last accessed: 20 November, 2018).

privacy on cyberspace not only to protect the individual's right but also to protect the national security and international peace. Right to privacy is well recognized in national and international instruments. It is need of the hour to protect the right to privacy of Individuals. The next chapter analyses the privacy as a right and evaluates the international legal framework of right to privacy.

Chapter Two

The Development of the Concept of Right to Privacy: An International Perspective

Introduction

This chapter focuses on the development of the concept of right to privacy from an international perspective and analyses international legal framework about right to privacy. It also considers the emergence and development of the right to data privacy and its legal protection, especially, under international law. This Chapter is divided into five Sections. Section one defines the concept of right to privacy. This section examines what privacy is, and how different definitions of privacy constitute different approaches to privacy protection. Section two discusses the development of the philosophy of the right to privacy. Section three discusses kinds of privacy, namely, physical privacy, informational privacy and organizational privacy. Section four analyses the provisions of HRL. In this respect, it analyses provisions of the Universal Declaration on Human Rights (UDHR) 1948, International Covenant on Civil and Political Rights (ICCPR) 1966, Convention on the Rights of Child (CRC) 1990 and the International Convention on the protection of the rights of all Migrant workers and members of their families (ICRMW) 1990. Further, it analyses the judicial opinions on privacy including the decisions of the American Courts, European Court of Human Rights (ECHR), Supreme Court of India and Inter-American Court of Human Rights (IACHR). Section five describes the Islamic concept of right to privacy.

2.1 Definition and Concept of Right to Privacy

The origin of the word "Privacy" is a Latin term "Privatus" which means "to be separated from others". Privacy is the ability of a person or persons to segregate themselves and their data from intrusion. The expression "privacy" has been portrayed as "the legitimate wish of a person to expose himself with others in his desired way". Privacy also includes the control of an individual over the time, place and conditions which he wants to communicate with others. Moreover, it also deals with his right to wave or to continue as he deems fit. It additionally implies the person's entitlement to control dispersal of data about himself as it is his very own property. Privacy has been discussed as a Zero-relationship between two or more persons as there is no connection between them.

A number of rationalists have favoured the privacy as it fulfills a lot of essential human needs. The limits and substance of privacy differ among societies, cultures and people. Privacy may be a desire to stay unnoticed or unidentified in a society. How much private data is to be uncovered relies upon the idea that how general society will get this data. Privacy can be viewed as a part of security in which one exchanges such information which he thinks to be secure for himself.[95]The notion of privacy is connected with western society specifically with England and North America. Some researchers believe that the right to privacy is stemmed out from Anglo-American culture separated from other Western European societies.[96] Privacy laws are made by various nations but these laws themselves put certain limitations to the right to privacy. Such as

[95] Solove, Daniel J. "Understanding privacy." (2008).
[96] Walia, Ivneet Kaur. "Infringement of Right to Privacy as a Crime." *Available at SSRN 1591081* (2010).

taxation laws require information about the property, wages and profits of an individual. Similarly, in some countries "Privacy" may be contradicted with freedom of speech or freedom of expression.

In some countries, the information about a certain matter belonging to a particular person may be deemed public but the same may be treated and secured as private in other culture or society. Many academicians who are financial experts, scholars, and research psychologists depict privacy as a 'willful forfeit', or 'voluntary sacrifice'. In business era an individual may compromise his privacy in order to win a prize or for advertising purpose. A data which is shared willfully and later on it is stolen or abused may be end into various identity frauds. The nature, scope and extent of privacy is divergent regarding how much protection a man is qualified for? or what amounts an attack to privacy?[97]

David Flatherty, asserts that the technology advancement extended the scope of privacy. He recognized the data protection and privacy of information as a right. He holds that the information must be controlled and limited to keep privacy. Furthermore, he argues that the people are needed to be allowed to remain unbothered and to control how the information is used about them.[98] Richard Posner and Lawrence Lessing's debated on the financial domain of individual's data and his control over the flow of data. According to Posner, it is not good to control such data which lessens the productivity of a business. He says business is offering oneself in the work and advertising of which is equal to marketing of an item and any concealment of such information about business is a fraud.[99] According to Lessig, online breach of privacy can be managed by law

---

[97] Ibid;

[98] David Flaherty, *Protecting privacy in surveillance societies: The federal republic of Germany, Sweden, France, Canada, and the United States.* Chapel Hill, The University of North Carolina Press, United States, (1989).

[99] Posner, "The economics of privacy", *The American Economic Review*, (1981): 405-409.

and practice. He believes that the privacy and protection would be more strengthened if individuals are more capable of controlling information about themselves.

Many endeavors have been made to recognize the privacy as a significant human right which is most important to govern the system of a democratic state. Various strategies have been adopted by philosophers to explain this right beyond the ambit of individuals liberty. Amitai Etzioni, recommended the communitarian way to deal with this right to privacy which requires a good culture to maintain this need. He holds the opinion that privacy is a good thing among numerous others and it relies upon network responsibility. He asserts that privacy laws rise the need to control government observation and surveillance.[100]

According to Priscilla Regan, an individual's idea of privacy has failed logically and keep no existence in policy. She is in the favour of social estimation of privacy. She believes that privacy contains three dimensions namely shared perceptions, public values, and collective components. Shared ideas permit freedom of conscience and multiplicity in thinking approach. Public values ensure independent and fair participation along with freedom of speech and association as well as control government powers to peep into individual's life. Collective components support privacy as collective benefit. Regan focuses on policy making to achieve good privacy. According to her if a state is able to recognize the public-good value of privacy, it can attain the maximum of protection and security of its individuals.[101]

Leslie Regan Shade, believes that right to privacy is the necessity to acquire human pride and self-sufficiency. Privacy is maintained upon standards for how data is shared and if it is proper

---

[100] Etzioni, "A communitarian perspective on privacy", *Connecticut Law Review*, (2000): 897-905.
[101] Regan, "Legislating privacy: Technology, social values, and public policy. Chapel Hill", The University of North Carolina Press, United States, (1995).

or not. Infringement of privacy is attributed to the policies which deal with privacy and data protection. The UDHR, 1948 asserts that "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[102]

Finally, privacy in cyberspace may be labelled as an individual's right to secure his personal information as a property right that is alienable and, in this way, one might lose his data. Privacy is also depicted as a collective esteem and human right. In the era of technology and the world of property rights administration, a conflict may be occurred between political powers and individual's privacy right. This blend of two may be accomplished by freedom of speech, rule of law and morality. [103]

2.2 Development of the Philosophy of Right to Privacy

The concept of individual's safety in person as well as the security of his property is as old as the common law itself. However, it requires occasionally the reassuring of this need. Because of various political, social and financial changes, new laws are designed to meet the needs of society. Initially "the law gave a cure only for physical intrusion with life and property". The "right to life" meant just to shield the person from battery of different types. Liberty was attributed with freedom from definite restraints and limitations while right to property was limited to one's territories and his cattle's. Afterwards, the intellectual instinct of a person was also perceived and acknowledged. In this way new laws and rights were established. Now "the right to life has been expanded to the right to enjoy the life, the right to be let alone, the right to be not identified or to live

[102] http://www.un.org/Overview/rights.html>, (Last accessed: 20 November, 2018).
[103] http://en.wikipedia.org/wiki/Kristo_Ivanov> (Last accessed: 20 November, 2018).

unmentioned".[104] The right to property has been broadened to the possession of every form of property whether tangible or intangible.

The right to privacy can be characterized as a vital human right. It can be traced from the history as far back as 1361 from the provision of Justice and peace Act of England, when the arrest was ordered for peeping toms.[105] In 1765, a British Lord Camden stroke down a warrant to go into a house and seize papers by stating that we can assert that there is no legal remedy to secure the litigants for what they have done and if there could be any law it would only destroy the social lives of persons as the papers may be the most important property as a person may have.[106] According to William Pitt, a parliamentarian, "The poorest man may in his cabin offer disobedience to all the power of the Crown. It might be fragile; its rooftop may shake; the breeze may blow it; the storms may enter; the rain may enter; yet the King of England can't enter; every one of his powers could not dare to cross the limit of the demolished apartment".[107]

Different nations established particular insurances for privacy in the different times. In 1776, the Swedish Parliament sanctioned the "Access to Public Records Act" which necessitated that all government held data shall be used for lawful objectives only. In 1792, the Declaration of the Rights of Man and the Citizen, proclaimed that private property is sacred. In 1858, France denied the production of private data and set certain penalties for violation.[108] As privacy is based

---

[104] Brandeis, Louis, and Samuel Warren. "The right to privacy." *Harvard law review* 4, no. 5 (1890): 193-220.

[105] Jeanne M. Hauch, "Protecting Private Facts in France: The Warren & Brandeis Tort is Alive and Well and Flourishing in Paris", 68 *Tul. L. Rev.* 1219 (May 1994).

[106] *Entick v. Carrington*, 1558-1774 All E.R. Rep. 45.

[107] T.D. Nova, "The future face of the worldwide data privacy push as a factor affecting Wisconsin businesses dealing with consumer data", 22(3) *Wisconsin International Law Journal.* (2004): 792.

[108] Jeanne M. Hauch, "Protecting Private Facts in France: The Warren & Brandeis Tort is Alive and Well and Flourishing in Paris", 68 *Tul. L. Rev.* 1219 (May 1994).

on the natural rights and therefore is connected with ITs and data protection. In 1980s, the US Supreme Court, Justice Louis Brandeis explained the privacy as an individual's right 'to be let alone'.[109] This assertion was made in reaction to the advanced technologies and new modes of information in form of photography and newscasting. Warren and Brandeis pronounced that the data which was covered and private in past is presently yelled from the housetops. Privacy rights are knotted by data innovation and technologies inventions.

Olmstead's dissent was generated in 1928, "when he wrote 'Subtler and more far-reaching means of invading privacy have become available to the Government'".[110] Development has made it possible for Government to perceive what is whispered in court. By 1967, phones were turned out to be close to gadgets "with lines not shared over homes and exchanging was made electro-mechanical". "New processing and recording innovations started to raise worries about security which brought the Fair Information Practice Principles in the 1970s".[111]

The pioneer privacy yardstick at a global level is the UDHR, 1948 which particularly ensured regional and communication' privacy in its article 12.[112] Various universal human rights agreements give particular reference to protection of privacy as a right. The ICCPR, the ICRMW[113] and the CRC[114] provide a similar notion of privacy. At the regional level efforts have been made to protect the privacy as a matter of right. These rights are made enforceable. The Convention for

---

[109] Samuel Warren and Louis Brandeis, "The right to privacy", *Harvard Law Review* 4, (1890): 193-220.
[110] *Olmstead v. United States.* 277 U.S. 438 (1928).
[111] Samuel Warren and Louis Brandeis, "The right to privacy", *Harvard Law Review* 4, (1890): 193-220.
[112] It states that: "No-one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks".
[113] A/RES/45/158 25 February (1991), Article 14.
[114] UNGA Doc A/RES/44/25 (12 December 1989) with Annex, Article 16.

the Protection of Human Rights and Fundamental Freedoms Rome 1950, Article 8[115] states: (1) "Everyone has the right to regard for his private and family life, his home and his correspondence". (2) "There shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health of morals, or for the protection of the rights and freedoms of others".

To administer the enforcement of privacy, European Commission of Human Rights and the ECtHR were established. Both have been observed dynamic in the implementation of privacy rights and to ensure its Articles.[116] It was held by the Commission that: "For numerous Anglo-Saxon and French authors, the right to respect "private life" is the right to privacy, the right to live, as far as one wishes, protected from publicity. In the opinion of the Commission, however, the right to respect for private life does not end there. It comprises also, to a certain degree, the right to establish and develop relationships with other human beings, especially in the emotional field for the development and fulfilment of one's own personality.[117] Many member states have been penalized by the court for neglecting to manage wiretapping from governments and private persons.[118] It has additionally noticed the instances of people' access to their own data in government documents to guarantee that satisfactory procedures were adopted.[119] It has extended

[115] Convention for the Protection of Human Rights and Fundamental Freedoms Rome, 4. XI. (1950).
[116] Nadine Strossen, "Recent US and Intl. Judicial Protection of Indvidual Rights: A comparative Legal Process Analysis and Proposed Synthesis", 41 *Hastings L.J.* 805 (1990).
[117] "For numerous "Anglo-Saxon and French authors, the right to respect "private life" is the right to privacy, the right to live, as far as one wishes, protected from publicity".
[118] *X v. Iceland*, 5 Eur. Commin H.R. 86.87(1976).
[119] ECtHR, "Case of Klass and Others: Judgement of 6 September 1978", Series A No. 28 (1979). "Malone v. Commissioner of Police", 2 All E.R. 620 (1979).

the scope of Article 8 from government activities to those of private people where the government has precluded these activities.[120] In this way the court may demand implementation of information insurance laws if it seems that the information was inappropriately handled.[121]

American Convention on Human Rights (ACHR), 1969 in its Article 11 ensures the right to privacy in wording like the UDHR.[122] The Organization for American States announced the American Declaration of the Rights and Duties of Man in 1965. This Declaration ensured the right to privacy along with many other rights.[123] The Inter-American Court of Human Rights (IACHR) also secured the right to privacy in its cases. According to Alan Westin new advancements have changed the harmony of privacy and revelation that may restrain government to ensure democratic processes. Westin explains privacy as "the choice of people, gatherings, or organizations to decide for themselves when, how, and to what degree data about them should be imparted to others". Everyone is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others, in the light of environmental conditions and social norms set by the society in which he lives. Alan Westin, in his Liberal Democratic Framework, "Privacy and Freedom, 1968" provides an opportunity for privacy to be isolated from political interference and ensures individual's independence while at the same time guaranteeing them the liberty of association and expression.

---

[120] Judgement of 26 March 1987 (Leander Case).

[121] Rolv Ryssdal, "Data Protection and the European Convention on Human Rights in Council of Europe Data protection, human rights and democratic values", XIII Conference of the Data Commissioners 2-4 October 1991 41-43, (1992).

[122] Signed Nov. 22, 1969, entered into force July 18, 1978, O.A.S. Treaty Series No. 36, at 1, O.A.S. Off. Rec. OEA/Ser. L/V/II.23 dec rev. 2.

[123] O.A.S. Res XXX, adopted by the Ninth Conference of American States, 1948 OEA/Ser/. L./V/I.4 Rev (1965).

Due to the emergence of ICTs, people have been entered into a virtual world. They have dependent on devices and internet. Information age and digital era have made human beings more social. Now, people communicate with each other every moment on smart phones and screens from thousands of miles distance. They make contracts with their business partners on virtual papers. They do their trades in digital centers. They shop their articles on Daraz, Amazon and Alibaba. They meet with their friends on Facebook, chatrooms, mailbox, WhatsApp and messenger. They order their meal on food panda and other online hotels. All these advancements of technologies made the mankind more vulnerable to security threats of privacy. The dependency on internet elevated the risks of intrusion in information and security.[124]

With the advent of smart technologies and internet, the individuals' privacy has become a target for intrusion. Many threats have generated to personal information and data. People use internet and information technology for ease but in return they have to pay back in shape of privacy invasion. This is digital era and smart technologies have become inevitable. The giant of virtual world stores all information and data of individuals. Time, date, distance, source, nature and kind of communication can be recorded. Threat to privacy of human beings has made it more challenging for lawmakers to make and provide a legal forum. Governments are trying to make policies to control cybercrimes and to protect individuals from privacy invasion.[125] According to the suggestions of Wikipedia, people may control privacy intrusion on internet. It is recommended that online information is collected from individuals by filling fake forms, unnecessary surveys,

[124] Rohit K. Gupta, "An Overview of Cyber Laws vs. Cyber Crimes: In Indian Perspective", Online available at: www.mondaq.com (Last accessed: 20 November, 2018).

[125] V. Godse, "Building an Ecosystem for Cyber Security and Data Protection in India". In: Kumar A., Zhang D. (eds) Ethics and Policy of Biometrics. ICEB 2010. Lecture Notes in Computer Science, vol 6005. Springer, Berlin, Heidelberg, (2010).

registrations and reports. Such type of information is used for committing cybercrimes related to financial loss by credit cards numbers, bank accounts, passwords and much more. Children and adolescences are the easy and favourite target for such intrusions into privacy.[126]

2.3 Types of Privacy

Privacy protection can be divided into various boundaries according to the invasion into the individual's matters. It can be segregated into following aspects.[127]

2.3.1 Physical Privacy

As it is shown by its name physical privacy means the stopping of interruptions into one's physical space or isolation. It also includes averting of private acts or one's body from being seen by others to maintain decency. It includes video tapes containing personal acts, practices or body parts, undesired searching of one's personal belongings, unlawful access to one's home or vehicle or unauthorized one's health related to medical decision without expert opinions or one's therapeutic choice.

An illustration of physical privacy is the US Fourth Amendment which recognizes the right to privacy of individuals. It states that people should be secured in persons, houses, papers and unauthorized forfeitures, seizers and searches.[128] Many countries including Pakistan have laws about trespass of property. Physical privacy varies from society to society and culture to culture. One may more sensitive in one matter of privacy as a safety of person or information.[129]

---

[126] Central Monitoring System (2014) in the Wikipedia: The Free Encyclopaedia, online available at: http://en.wikipedia.org/w/index.php (Last accessed: 20 November, 2018).
[127] http://en.wikipedia.org/wiki/Privacy> (Last accessed: 20 November, 2018).
[128] Andrew Dunlop, "Fixing the Fourth Amendment with trade secret law: A response to Kyllo v. United States". retrieved from < http://findarticles.com/p/articles/mi_qa3805/is_200206/ai_n9109326/> (Last accessed: 20 November, 2018).
[129] http://www.privacyrights.org/fs/fs14a-stalking.htm> (Last accessed: 20 November, 2018).

2.3.2 Informational Privacy

This domain of privacy deals with data and information provided on communication technologies and internet. It includes the mode of transfer of information as well as use of information. It is the gathering and sharing of one's personal information on digital devices. One may use such device for the purpose of transfer of information or to get some service or to provide some business. Such information and data may be accessed by some unauthorized person or may be reached in the hands of some criminals. In some situations, such information may be used to commit fraud or to commit crime against innocent persons. Technology must be assessed before sharing of data. How information is gathered and distributed for fraudulent purpose also matters. For such reasons one may be reluctant to rely upon these devices or to share information about his religion, beliefs, gender, political affiliations and associations.

Financial transactions are also important in this regard. One's personal information of his income, property or tax payments may be traced from his data that has been provided to some insurance organizations. It may also be trapped to commit fraud or some other purposes like to offer some product, policy medication or tourism. Similarly, internet information may be traced to know about an individual's interests, beliefs and activities. It is followed by personal history of a person's searches on internet. Another thing is the websites which might themselves gather and retain information from a person's visit to the site.

Medical privacy may also be interfered by tracking a person's medical visits to hospitals or calendrers for follow ups. It may also be infringed by collecting and using an individual's data that has been provided to health insurance companies or to some drug stores. It may affect a person's health privacy if he is not desirous to share his physical or mental health with others.

Sexual privacy also exists there which provides privacy of various matters related to the choice and selection of one's partner or to make relation with the persons of other region believes and sometimes even includes homosexuality. It keeps a man away from being compelled to carry a pregnancy to term and empowers people to obtain and utilize contraceptives and safe sex supplies without any breach of privacy or being reviewed by legal authorities or society.

Political privacy also become an issue to be addressed with the recognition of voting system. People demand fair elections without any intrusion to their political associations.[130]

2.3.3 Organizational Privacy

Different institutions, corporate bodies, associations, Government offices and agencies may wish to keep their certain acts and practices to be secret from other institutions, organizations and persons. To keep their information protected and secured these organizations may adopt certain ways including legal privileges and immunities. Like a government institution may announce certain information and data to be secret and prevent it to become public. Similarly, a government body may also seek some legal remedies to keep information protected.[131] A corporation may also demand privacy regarding its trade matters. Corporations and organizations may also practice privacy to maintain their standards in order to meet competitions.[132]

2.4 International Human Rights Law on Right to Privacy

The right to privacy is also guaranteed in international and regional HRL and it is assured that the universal framework must be of such type which may address any interference in individual

[130] http://en.wikipedia.org/wiki/Information_privacy> (Last accessed: 20 November, 2018).
[131] Vikram David Amar, "Executive Privilege: Often Valuable to Protect the Presidency, But Misunderstood By President Bush in the Condoleezza Rice Case", Retrieved from http://writ.corporate.findlaw.com/amar/20040416.html (Last accessed: 20 November, 2018).
[132] http://en.wikipedia.org/wiki/Kristo_Ivanov> (Last accessed: 20 November, 2018).

in individual's privacy by various institutions and companies. Government should take measures to stop such interference and make proper laws in this regard.[137]

In its general comment No. 16, the Human Right Committee (HRC) has underlined that "Correspondence should be delivered to the addressee without interception and without being opened or otherwise read".[138] Furthermore, the authors of the report noted that "focusing on controlling the collection and retention of personal data, while important, may no longer be sufficient to protect personal privacy", in part because "big data" enables data to be used as a new, non-obvious, unexpected forms of data".[139]

Another thing that is related to the privacy is the "metadata", in which the information is used in desired manner. In this situation the provided information is converted for some other purposes that has not been consented by individuals. Like health care providers may obtain data from drug stores to ascertain the record of purchase or to access the financial condition of a customer. European Union Court of Justice recently observed that "metadata", taken as a whole may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained.[140] Such collection or retention of communication data amounts to interference into privacy whether or not this data is subsequently used or consulted.[141]

---

[137] Ibid;

[138] "Official Records of the General Assembly, Forty-third Session", Supplement No. 40 (A/43/40), annex VI, para. 8.

[139] "Executive Office of the President of the United States". "Big Data: Seizing Opportunities, Preserving Values". May, (2014) (Online available and retrieved from: www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf), (2014): 54.

[140] "Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others", Judgment of 8 April 2014, paras. 26-27, and 37.

[141] Judgment of ECHR, *Weber and Saravia v. Germany*, para. 78; *Malone v. UK*, para. 64.

Who is allowed to Access Data and Information?

Interference into one's right to privacy is only allowed if it is not unlawful or it is justified by legal provisions. Otherwise, unlawful and arbitrarily interference with data and communication or information is totally forbidden. In its general comment No. 16, the HRC explained that the term "unlawful" implied that no interference could take place "except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant".

The expression "arbitrary interference" can also extend to interference provided for under the law. The introduction of this concept, the Committee explained, "it is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances". Article 17 of ICCPR provides the limitation on privacy rights. This limitation must be used lawfully and under unavoidable circumstances. It must be sure that only lawful surveillance is done for legitimate with least intrusion in privacy.[142] If limitations don't fulfil these requirements then it will be unlawful intrusion. In assessing the necessity of a measure, the HRC, in its general comment No. 27, on Article 12 of the ICCPR, stressed that that "the restrictions must not impair the essence of the right [...]; the relation between right and restriction, between norm and exception, must not be reversed."[143]

In some situations, it is required from states to access data particularly the records from telephone companies and internet service providers for national security concerns. It is directed by

[142] CCPR/C/21/Rev.1/Add.9, paras. 11 – 16.
[143] Judgment of ECHR, in *Handyside v. the United Kingdom*, para. 48; and *Klass v. Germany*, para. 42.

government to retain such data for access of certain intelligence agencies.[144] A review of national practice in government access to third-party data found "when combined with the greater ease with which national security and law enforcement gain access to private-sector data in the first place, the expanding freedom to share that information among agencies and use it for purposes beyond those for which it was collected represents a substantial weakening of traditional data protections."[145] In many states, judiciary has discouraged the practices of data collection and its surveillance with the help of judicial review to protect the fundamental rights of citizens. Some states have adopted measures to comply with limitations imposed by article 17 of the covenant.[146]

2.4.1 United Nations Declaration of Human Rights, 1948

This is the most significant document which spoke about privacy as a key fundamental right. Article 12 of the UDHR, 1948 addresses the right to privacy of an individual. This declaration requires the member states to make such domestic laws which may protect the privacy of their people. The identity of a person, his family and home are inviolable and must be protected from intrusion. This Article imposes a duty on a state that the privacy of a citizen must not be infringed except in accordance to the lawful procedures. The honour and repute of a person should be safeguarded from intrusion.[147]

2.4.2 International Covenant on Civil and Political Rights, 1966

Like UDHR, this covenant is also important for guaranteeing the right to privacy to individuals.[148] Article 17 of this covenant deals with right to privacy. Article 17 ensures the privacy of individuals

---

[144] CCPR/C/USA/CO/4, para. 22.
[145] Fred H. Cate, James X. Dempsey and Ira S. Rubinstein, "Systematic government access to private-sector data", *International Data Privacy Law*, vol. 2, No. 4, (2012): 198.
[146] Resolution A/HRC/14/46, annex, practice 23.
[147] Article 12 of UDHR, (1948).
[148] Article 17 of ICCPR, (1966).

in the like manner of article 12 of UDHR. Pakistan ratified this document in 2010 with few reservations which are not related to the right to privacy. The same provisions of Article 12 of the UDHR, 1948 are adopted in this covenant to secure the right to privacy.[149] Article 17 of this covenant explicitly deals with right to privacy. The same provisions of article 12 of the UDHR, 1948 are adopted in this covenant to secure the right to privacy[150], which states:

a. Nobody will be made subject to arbitrary or illegal interference with his privacy, Illegal attack on family, home or correspondence, or her honor and Prestige.

b. Everyone has the right to preserve the law against such interference or attacks.

As a multilateral treaty, the covenant is directly binding on its member states. In form of December 2003, there were 151 parties for the covenant, which means the right to privacy, inherent in it; has been adopted universally.

In 1988, the Human Rights Committee (HRC), a body built by the covenant regarding the implementation and enforcement of privacy, issued a general comment on the scope of article 17.[151] In the view of the Committee, Article 17 is not only a negative liability on state parties to not interfere with "arbitrary" or "illegal" privacy, but there is also a positive obligation on the state parties to implement measures for safeguarding the safety of the people. By violating their privacy from both private and public actors, in the words of Committee: "There is a need to guarantee this right against all such interference and attacks whether they came from state officials or natural or legal persons. In the obligations imposed by this article, the State requires legislative and others to

[149] Article 17 of ICCPR, (1966).
[150] Article 17 of ICCPR, (1966).
[151] General Comment 16, April 8, 1988, Official Records of the General Assembly, Forty Third Session, Supp. No. 40, UN Doc A/43/40, Annex, 181-183.

adopt measures to affect such interference and prohibition against attacks at the same time there is also the protection of this right".[152]

In addition, the committee strengthened the force and broadened its scope provision by separating concepts of "arbitrary" and "illegal" intervention. In her view, "illegal intervention" is what is not authorized by law, while "Arbitrary interference" is what is authorized by law but still violates Convention. It explains: "The purpose of the concept of arbitrariness is also to guarantee that intervention the provisions provided by law must be in accordance with the purpose of the covenant and in any event, should be appropriate special situation".[153]

In the context of the clear scope of the provision, the committee expressly stated that the security of the article extends to the individual's personal information. Collection limits, clarifying the basic data protection principles of privacy, objectives specification, accuracy and accessibility committee said that: "Effective measures are to be taken by the states to ensure that information regarding the personal life of a person who does not reach the hands of those people it has been authorized by law to obtain, process and use, and it is never used for purposes. Incompatible with the covenant so that the most effective protection possible his personal life, every person should have the right to know smarter form, whether, and if so, is personal data stored in automatic data files, and for what purposes. Everyone should also be able to find out which public authority or private person or body can control their files. If such files contain incorrect personal data or contrary to the provisions of the law, collected or processed, each person must have the right to request improvement or abolition".[154]

---

[152] Ibid., para. 1.
[153] Ibid., para. 4.
[154] Ibid., para.10.

2.4.3 Convention on the Rights of Child, 1989:

This convention was adopted to protect the rights of a child. Article 16 of this convention is related to the child's right to privacy. It is worth mentioning here that a child's right to privacy is secured in the same manner as of an adult. It is clearly stated in the said provision that a child shall be protected in the same way as an adult; the child's privacy is equal to an adult person. Moreover, the family, home and the other communications of a child shall also be protected from unlawful intrusions. Similarly, the privacy of a child is also liable to be protected from any interference by law.[155] Child pornography on cyberspace also comes within this context and it is the privacy infringements if any such activity is carried on. This convention is a milestone to ensure the right to privacy of a child. This convention grants the child with same equal status of privacy as an adult have. According to article 16 of the convention a child has the protection against unlawful interference in his privacy, family, honour and reputation.[156] Further, this article also gives the right to a child to seek legal protection against such intrusion of privacy.[157] Pakistan ratified it on December 12, 1990. By such ratification the children in Pakistan also have the same protection of law against the infringement of his personal or family privacy.

2.4.4 International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (ICRMW), 1990:

This convention talks about the rights of the migrant persons. It is an important convention as it discusses the new venue of privacy. It states that the privacy of migrant persons shall be saved in

[155] Article 16 of CRC, (1989).
[156] Article 16(1) of Convention on the Rights of Child.
[157] Article 16(2) of Convention on the Rights of Child.

the same manner as to the citizens of a state to which they have been migrated.[158] In this situation it is the duty of a state to protect the rights of all persons who reside in it whether they are its citizens or not.

2.4.5 Regional Human Rights Laws on Right to Privacy:

Like international human rights some regional efforts have been made by various states to protect the privacy of individuals.

American Convention on Human Rights (ACHR), 1969:

This convention was adopted in 1969. This convention has the similar provisions for the protection of privacy as mentioned in the UDHR and the ICCPR. The convention provides that no one shall be interfered with his personal life or his family life or his home or his correspondence arbitrarily or abusively. It further restricts the unlawful damage and attack to a person's honour and reputation. It further shelters a person by providing the equal protection of law against abusive and arbitrary interference and intrusion into the privacy of a person or his family or house.[159]

European Convention for the Protection of Human Rights (ECHR) 1950:

This convention was adopted in 1950. It addresses the privacy as a right in its Article 08. It states that the privacy of a person, his family, his home and his communication is liable to be protected from intrusion. Similarly, it also forbids the unlawful and illegal interference into the privacy of a person. However, it compromises this right to privacy on the grounds of state security, national interest, foreign relations and public order.[160]

---

[158] Article 14 of ICRMW, (1990).
[159] Article 11 of ACHR, (1969).
[160] Article 08 of ECHR, (1950).

2.4.6 Judicial Opinions on Privacy:

2.4.6.1 Decisions of Courts of the USA:

The American constitution does not provide the free steering of right to privacy for its citizens. However, the supreme Court has delivered its decisions in favour of right to privacy on the basis of Bill of Rights. These decisions are related to the invasion of privacy in the areas where people expect that they have reasonable privacy from any surveillance[161] , or in the issues of marriage, family relationship, procreation, education or use of contraceptive pills.[162] The Supreme Court also endorsed the right to privacy of political groups to disclose the name of their members to government agencies.[163] In *Reno v. Condon*, the Supreme Court decided that the information provided by drivers to motor vehicle companies is the piece of commerce and should be monitored by the federal government to protect the privacy[164]. In *kyllo v. United States,* the Supreme Court held that a thermal imaging drive without the search warrant is unconstitutional and illegal[165]. The Supreme Court declared it unconstitutional in the light of Fourth Amendment which is related to the protection of intrusions[166]. Supreme Court also restrict a hospital that it cannot make any diagnostic test without the consent of the person and it is against the right to privacy and liberty of an individual.[167]

In *Lawrence v. Texas,* the Supreme Court struck down the legislation of a state that prohibited the homosexual relation. The Court held that it is in violation of due process rights of

---

[161] *Katz v. United States*, 386 U.S. 954 (1967).
[162] *Griswold v. Connecticut*, 381 US 479 (1965); *Whalen v. Roe*, 429 US 589 (1977).
[163] *NAACP v. Alabama*, 357 US 449 (1958).
[164] *Reno v. Condon*, 528 U.S. 141 (2000)
[165] *Kyllo v. United States*, 533 U.S. 27 (2001).
[166] *City of Indianapolis v. Edmond*, 531 U.S. 32 (2000).
[167] *Ferguson v. City of Charlestown*, 532 U.S. 67 (2000).

constitution.[168] Justice Kennedy in this regard asserted that the petitioners are respected for their private conduct. The Court has no jurisdiction to question their private sexual conduct.[169] This was stated in line of the decisions of the ECHR and other foreign Courts about the homosexual rights of adults.

2.4.6.2 The Inter-American Court of Human Rights (IACHR):

The IACHR supported the right to privacy in a large number of cases. The court decided in the case of *Fontevecchia & D'Amico v. Argentina*[170], that the publication related to the former president of Argentina is not the infringe of the right to privacy. It was the opinion of the court that the information was already well known to the public and it was also a matter of public interest. So, the publication of any information related to Menem is not the intrusion into his privacy. In another case of *Tristan Donoso v. Panama*[171], the Inter-America Court amounts it the infringement of right to privacy when the private conversation of telephone was transferred to the church officials and member of bar association. This conversation was made by private parties and the right to privacy was violated through the transfer of such information without the consent of the subject.

On another occasion the court also supported the notion of privacy in *Escher et al. v. Brazil* case.[172] In this case the court also asserted that the burden of proof in the context of telephone surveillance does not lie upon the complainant because of his inconveniency to proof the facts. A

[168] 58.539 U.S. (2003), para. 02-102.
[169] Brief amici curiae of Mary Robinson, Amnesty International USA, Interights, "the Lawyers Committee for Human Rights, and Minnesota Advocates for Human Rights", HRW, online available and retrieved from: http://www.hrw.org/press/2003/07/amicusbrief.pdf. (Last accessed: 16 November, 2018)
[170] 29 November, (2011), Series C, No. 238.
[171] 27 January, (2009). Series C, No. 193, para. 83.
[172] 6 July, (2009), Series C, No. 200, paras. 127-128.

complainant is exempted to proof these facts because of security measures adopted by a state to collect the information and data.

2.4.6.3 European Court of Human Rights (ECtHR):

The ECtHR also supported the right to privacy in its various judgments. The court highlighted the numerous of state practices as an intrusion into one's right to privacy. Such as the tapping of telephone conversations[173], intrusion into sexual life[174], forced medical treatments[175], access to state-held information[176] and distribution of rights for children.[177] In the case of *Von Hannover v. Germany*, the court decided that the privacy also includes the person's name, his physical image, his physical and psychological integrity as well. A person's personality is amounted to privacy from other human beings.[178] In the case of *Niemietz v. Germany*[179], the court held that the privacy cannot be restricted only to one's personal life without the interaction from another person. It involves some degree of compromise related to sharing of information like business community.

However, a person cannot exclude the whole world from his sphere of privacy. In the case of *Keegan v. Ireland*[180], it was decided by the court that a wide range of privacy may be applied while adopting a child. As in the said case the father wanted the guardianship of a child whose mother was separated from him and seeking adoption of the child. Further, the court decided in the case *Murray v. the United Kingdom*[181], that the collection of any information and data upon

---

[173] *Iordachi and Others v. Moldova*, 10 February, (2009), Application No. 25198/02.
[174] *Dudgeon v. the United Kingdom*, 22 October, (1981), Application No. 7525/76.
[175] *Acmanne and others v. Belgium,* 10 December, (1984), Admissibility Decision, Application No. 10435/83.
[176] *Gaskin v. United Kingdom*, 7 July, (1989), Application No. 10454/83, paras. 41 and 49.
[177] *Elsholz v. Germany*, 13 July, (2000), Application No. 25735/94.
[178] Application No. 59320/00, 24 June, (2004), para. 50.
[179] Application No. 13710/88, 16 December, (1992), para. 29.
[180] Application No. 16969/90, 26 May, (1994), para. 47.
[181] Application No. 14310/88, 28 October, (1994), para. 89.

the arrest of a person is the violation of the right to privacy except if such data is required in certain specific situations. Similarly, the court held in the case of *Leander v. Sweden*[182] that the collection and transfer of personal information without lawful reason is the violation of privacy. The court further stated that there must be adequate measures for the collection, retention and sharing of personal information.[183] In *Z. v. Finland*, it was held by the court that the disclosure of personal information about medical issue of a patient is the violation of private life.[184] In the said case the applicant claimed the infringement of his right to privacy through judicial process. The applicant was the patient with HIV positive. She pleaded that her name may be kept secret in the judgment. The court held that the sharing of information is the violation of privacy but the applicant was given reasonable opportunity of object that any part of information or of its use as evidence in criminal proceedings. However, the publication of the judgment may be made after omitting the name of applicant.[185]

In the case of *M.S. v. Sweden*[186], the court held that the disclosure of personal information by a public office is the violation of privacy. However, it also decided that the necessary information for the benefit of the person may be shared. In another case of *Leander v. Sweden*[187], the court concluded that the retention of personal information along with refusal of access by the subject is a violation of right to private life. It was also the opinion of the court that such refusal to review the information about oneself may be made in national interest. In the said case the Leander

---

[182] Application No. 9248/81, 26 March, (1987), para. 49.
[183] *Kruslin v. France*, 24 April, (1990), Application No. 11801/85, para. 33. para. 62.
159 Ibid; Kruslin v. France, 24 April, (1990), para. 35.
[184] Application No. 22009/93, 25 February, (1997), para. 94.
[185] Ibid; paras. 111-113.
[186] Application No. 20837/92, 22 August, (1997), para. 35.
[187] Application No. 9248/81, 26 March, (1987), para. 49.

was fired from job because of his political beliefs on the ground of state's security.

In *Gaskin v. United Kingdom*[188] it was held by court that the Gaskin, who was under supervision of local authorities of United Kingdom, being a child is liable to collect information about his childhood development and the refusal to such information is the breach to his private life. In *Guerra and Ors. v. Italy*[189] case is also related to the right to access of information related to one's private life. The court ordered that the Guerra must be informed about the pollution amount in the environment to protect his personal life.

Thus, in deciding these cases the court is of the opinion that the personal information about a person requires a great degree of protection in order to keep balance between freedom of expression and right to privacy. Moreover, the court also observed that the confidentiality of data and communications are of major concern. The collection and sharing of personal information may be made after due care and diligence.[190]

2.4.6.4 Supreme Court of India:

The Supreme Court of India in its judgments acknowledged the right to privacy. The constitution of India does not explicitly talk about the right to privacy. However, the Supreme Court asserted in its judgments that the right to privacy is adherent to the right to life and liberty. The right to liberty means the freedom to be not interfered. In its landmark judgment in the case of *Kharak Singh v. State of UP*[191], the Supreme Court of India foremost accepted that the right to privacy is inculcated in the Article 21 of the constitution.

---

[188] Application No. 10454/83, 12 EHRR 36. 7 July, (1989).
[189] Application No. 14967/89. 19 February, (1998).
[190] Application No. 2872/02, December, (2008), para. 46-50.
[191] AIR 1963 SC 1285

Article 21 states that no one shall be deprived of his life or liberty except according to the procedure established by law.[192] The Supreme Court stated that the liberty of a person also includes the right to privacy. In the said case the Supreme Court declared the visit of policeman into the petitioner's home as the invasion into the right of liberty and the violation of privacy. It further stated that the right to privacy is ancillary to the right of life but without any visible specification it remains in the grey area. The Supreme Court also elaborated the fundamental rights by struck downing the provisions of a Regulation related to the domiciliary visits of the suspect. However, some provisions of Regulations declared constitutional and not inconsistent to the freedom of speech and expression.

In *Gobind v. State of M.P*, the Supreme Court upheld the provisions of the Regulation related to the domiciliary visits of the security personal to monitor the activities of the suspect is not the infringement of a fundamental right. The right to privacy depends upon the certain restrictions of public interest and this right may be compromised according to the character and antecedent of the suspect. In *Mr. X v Hospital Z,* the Supreme Court held that it was the duty of hospital officials and doctors to unveil the information about the patient with HIV positive to a girl who intended to marry him. Such disclosure is not covered under the preview of right to privacy as the right to life of other person is on stake because of this information.

In the case of the *Peoples Union of Civil Liberties v. UOI, the Maneka Gandhi*[193] gave its worth remembering decision which established the status of privacy as a right. the supreme court held that the tapping of telephone is the serious invasion of the right to privacy of a person. It is

[192] *Kharak Singh v. State of UP*, 1 SCR 332 (1964).
[193] AIR 1997 SC 568.

the clear violation of the provisions of constitution. It is the infringement of the right of liberty that is preserved in constitution. After this landmark decision the wiretaps are considered as a serious invasion into privacy of persons.

In *R.Rajagopal v. St. of T.N.*[194] case, the supreme court decided that the right to privacy and the right to be let alone is mentioned in Article 21 of the constitution. No one can interfere into the life of a person, his family, home, marriage, procreation of children, motherhood and education. Moreover, it was also said by the court that no one can make the publications of these matters without the consent of the person. The court further held that the publication of such data is the violation of privacy of a person. It is also understood that the institutions are also not precluded to publish any data belonged to an individual without his consent. Delhi High Court sentenced the first cyber criminal in 2003. The court punished the criminal for making online cheating. The criminal stole the data from the credit card of an American citizen and used the information to order the colored television and a cell phone.[195]

2.5 Islamic Concept of Right to Privacy

The right to privacy is also explicitly provided in Islam. The concept of privacy does not allow any person to interfere into the life of other persons. Islam prohibits the people from entering into the house of others without the permission of inmates. The right to privacy is also enshrined in the Holy Quran. There are many verses in the Quran which says about privacy.

Allah says in the Quran that:

---

[194] 1994 SCC 632.

[195] www.hindustantimes.com/news/181_156334,0008.htm (Last accessed: 16 November, 2018).

"يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَدۡخُلُواْ بُيُوتًا غَيۡرَ بُيُوتِكُمۡ حَتَّىٰ تَسۡتَأۡنِسُواْ وَتُسَلِّمُواْ عَلَىٰٓ أَهۡلِهَاۚ ذَٰلِكُمۡ خَيۡرٞ لَّكُمۡ لَعَلَّكُمۡ تَذَكَّرُونَ "[196]

"O Believers, do not enter other houses than your own until you have the approval of the inmates and have wished them peace; this is the best way for you: it is expected that you will observe it ".

At another place it is said that that if you seek permission and no permission is granted to you then go back[197].

"فَإِن لَّمۡ تَجِدُواْ فِيهَآ أَحَدٗا فَلَا تَدۡخُلُوهَا حَتَّىٰ يُؤۡذَنَ لَكُمۡۖ وَإِن قِيلَ لَكُمُ ٱرۡجِعُواْ فَٱرۡجِعُواْۖ هُوَ أَزۡكَىٰ لَكُمۡۚ وَٱللَّهُ بِمَا تَعۡمَلُونَ عَلِيمٞ "[198]

"Then, if you do not find anyone therein, do not enter until you have been given permission, and if you are told to go back, you should go back. This is a purer way for you; and Allah has full knowledge of what you do ".[199]

"لَّيۡسَ عَلَيۡكُمۡ جُنَاحٌ أَن تَدۡخُلُواْ بُيُوتًا غَيۡرَ مَسۡكُونَةٖ فِيهَا مَتَٰعٞ لَّكُمۡۚ وَٱللَّهُ يَعۡلَمُ مَا تُبۡدُونَ وَمَا تَكۡتُمُونَ"[200]

"There is, however, no harm if you enter houses which are not dwelling places, but contain something useful for you ; Allah knows what you disclose and what you conceal."

Spying and suspicion into the matters of other persons are also forbidden by Allah.

"O ye who believe! avoid most of suspicions; for suspicion in some cases is a sin. And spy not on each other, nor back-bite one another. Would any of you like to eat the flesh of his brother who is

---

[196] The Holy Quran: Surat-Al-Noor, 24:27.

[197] Ali, Maulana Muhammad. *Holy Quran*. Ahmadiyya Anjuman Ishaat Islam Lahore USA, 2011.

[198] The Holy Quran: Surat-Al-Noor, 24:28.

[199] Ali, Maulana Muhammad. *Holy Quran*. Ahmadiyya Anjuman Ishaat Islam Lahore USA, 2011.

[200] The Holy Quran: Surat-Al-Noor, 24:29.

dead? Certainly, you would loathe it. And fear Allah, surely Allah is Oft-Returning with compassion and (is) Merciful."[201]

There are also many instances and practices enforced by the Holy Prophet (PBUH) to ensure the right to privacy of individuals. These practices set the defined rules and regulations for the person to live in a society.

It is narrated by Huzail bin Shurahbil that "a person came to Holy Prophet (PBUH) while standing in front of the door. The Prophet (PBUH) said to him that stand aside from the door". [202] It was the routine of the Prophet (PBUH) that He (PBUH) used to stand on left or right side of the door whenever He (PBUH) went to visit any person in his house. [203]

It is narrated by Sahl b. Sa'd as-Sa'id that once a person was peeping into the home of the Prophet (PBUH). At that time there was a comb in the hands of the Holy Prophet (PBUH). The Prophet (PBUH) said that if I could know that you are seeing into the house, I would shove this comb into your eyes. It is not only the entrance which is forbidden but also the glimpse that is also not allowed.[204]

Hadrat Abdullah bin Abbas reported that "the Holy Prophet (PBUH) said that whoever peeps into the letter of another person without his permission it is similar to glance into the fire". [205] In another tradition it is reported that the Holy Prophet (PBUH) said that whoever peeps into the house of another person then there will be no sin for you if you injure his eye with stone.

---

[201] The Holy Quran: (Surat-Al-Hujuraat, 49:12).
[202] Imam Abu Da'ud Book 41, Number 5155.
[203] Imam Abu Da'ud Book 8, Number 5167.
[204] Imam Muslim Book 025, Number 5366.
[205] Imam Abu Da'ud Book 8, Number 1480.

Similarly, it was said by the Prophet (PBUH) that there will be no punishment for you if you injure a person's eye while looking into yours home.[206]

In another narration it is reported that it is said by the Holy Prophet (PBUH) to seek permission from the inmates before entering into the house even if the resident is your mother or sister. It is reported by Sa'd bin `Ubadah that once the Prophet (PBUH) came to his home and sought permission thrice to enter into house. I replied in very low voice just to listen the sacred voice of Prophet (PBUH) for three times. After finding no permission He (PBUH) turned back. Then Sa'd came outside and ran to Him. He told the Prophet (PBUH) that he was answering in low voice to listen the Messenger of Allah.[207]

Cairo Declaration on Human Rights in Islam (CDHRI):

This declaration was adopted in 1990 by the member states of the Organization of Islamic Council (OIC). This declaration was adopted to discuss human rights in Islamic perspective. It is stated in this declaration that no person shall be discriminated on the basis of gender, race, colour, religion, belief and political association. Moreover, it also forbids the spying and intrusion into the privacy of a person as well as his home, his family and his conversations. It is also restricted that the home of a person shall be inviolable, and nobody is permitted to enter without permission or lawful authority.[208] This convention upholds the principles of UN Charter, UDHR and ICCPR. It also affirms the right to privacy in the same language of the said documents.

Pakistan signed this declaration in 1990. It ensures the security of an individual into various domains. It guarantees the protection of a person himself, his family, his home, his religious

[206] Imam Abu Da'ud, Book 41, Number 5153.
[207] Imam Abu Da'ud - Book 41, Number 5166a.
[208] Article 18 of CDHRI, (1990).

beliefs, his reputation, his property and other belongings and his communications. It also imposes restrictions on spying of one's activities. It argues that a person is free to deal with his private matters among his family in relation to his property and relationship. Moreover, it also forbids defaming the good name of an individual without any lawful authority.[209]

Conclusion

In this chapter the concept and development of right to privacy is examined. In this regard, the different international agreements are discussed which favour the privacy as a fundamental human right. Such as, UDHR, ICCPR and CRC explicitly talk about the privacy as an unavoidable human right. As the question of privacy protection in cyberspace is concerned, the United Nations along with other international and regional organizations is struggling to deal with this eminent issue with iron hands. Privacy in cyberspace must be considered as the Human Right, it must be endorsed by an international mechanism through which its protection may be ensured. Islamic teachings related to the right to privacy are also discussed. The condition of privacy has also been emphasised by the *Shari'ah* which is the root of the Pakistani legal system. It is concluded that proper legislation is required to deal with the security and protection of individuals' privacy in virtual world. The developed nations are trying to secure the information on cyberspace. For this purpose, the judicial opinions of various states are examined. It is also important to analyse the legal framework related to cyberspace and right to privacy of different nations. Therefore, the next chapter is incorporated to evaluate the cyber laws in USA, Europe, Australia and Asia.

[209] Article 18 of CDHRI.

Chapter Three

Development of Cyberspace Laws in America, Europe, Australia and Asia

Introduction

This chapter examines the cyberspace laws at international level by focusing on the legal framework of America, Australia, European countries and Asia. It analyses the current privacy laws and regulations which are applicable to telecommunications sectors in these countries. This Chapter is divided into five Sections. Section one examines the extent to which the right to privacy is protected and maintained in accordance with the US Constitution. It also investigates the US privacy legislation applicable to the public sector and to the telecommunications and banking industries in the private sector. Section two discusses about the legal frame work related to the right to privacy in different European countries. Section three addresses the cyberspace laws of Australia. While Section four deals with the cyber laws of Asian countries. Section five discusses about the emergence of data protection in Cyberspace Technology by considering privacy Regulations adopted by European Union (EU), the UN guidelines on data privacy, 1990 and the Asia Pacific Economic Cooperation (APEC), 2004. A good example of a legal system treating privacy as a human right is that of the European Union. The European Union is deemed the best approach to protect this right through the adoption of a comprehensive approach. Thus, the European Union introduced the Directive on the Protection of Personal Data, which expressly states that the right to privacy is a fundamental right and freedom of natural persons. It also discusses regional human rights laws and the role of South Asian Association for Regional Cooperation (SAARC). Further, it examines the role of UN Special Rapporteur on the right to privacy in cyberspace and the reports by the UN Rapporteur on the issue of cyberspace crimes.

3.1 Reason Behind Development of Cyberspace Laws

Due to the rapid growth of technologies the use of cyberspace has become indispensable. Many states have designed their defense and security policies according to the needs of time. These states have made legislation to keep cyberspace secure and to maintain the privacy of individuals.[210] These states have designed their cyber security strategies as counter measures to the threats in cyberspace. These counter measures are similar in three aspects. First, every state has its cyber security strategy to keep cyberspace free from threats and dangers. Second, public-private cooperation under the supervision of Government to enhance cybersecurity and develop interdepartmental coordination and third, the intervention of government into private sectors to impose cyber security policies and regulations.[211]

Some developed states in comparison to the developing states have more efficient code of cyber laws and policies. But because of its borderless and boundaryless jurisdiction it is a daunting task to safe and protect this environment from intrusion into information and privacy. However, the developed states are trying to cope this issue to provide a secure place in digital era. Another reason of this issue is incompatibility and non-cooperation of domestic laws with international laws. There is a great need to develop a universal pattern of cyberlaws to maintain a fear free, secure, confidential and perfect cyberspace. As the nature of virtual world is accessible to all individuals regardless of their territory and nationality; it is the responsibility of every state to develop cyberlaws to enhance its security.

---

[210] Kyoung-Sik Min, Seung-Woan Chai and Mijeong Han, "An International Comparative Study on Cyber Security Strategy", *International Journal of Security and Its Applications*, Vol.9, No.2 (2015):13-20 http://dx.doi.org/10.14257/ijsia.2015.9.2.02

[211] Ibid; at 21.

As national efforts towards the legislation for data privacy and protection is very wide and differs from country to country. This multitude of national legislation finally fashioned an international privacy regulatory patchwork quilt comprised of various constitutions, common laws and federal legislations of various states.[212] This divergency of data privacy regulation in national legislative framework abandoned the formation of a single international universal instrument on international level. Such single and uniform data privacy regulations are necessary for trade, commerce, banking and insurance industries to protect the data flow at international level among states. To survive a good legal framework for advantages, the states are required to formulate an even pattern of legislation in the light of international instruments. The regulations adopted by developed countries to protect the privacy of citizens are discussed here.

3.2 Cyberspace Laws in the USA

The Cyber Security Policy of the USA

To control the occurrence of cybercrimes and to protect the national security US has designed its policy. Current US cyber security is based on Comprehensive National Cybersecurity Initiative (CNCI). The CNCI was designed by Bush administration in 2008. Later on, in Obama's regime this policy was reviewed in 2009, known as Cyberspace Policy Review (CPR). [213] The CNCI is the core element to update the national cyber security of USA. It includes various dimensions to secure the cyber environment of country. The standards mandated to the various sectors include

[212] Report of Electronic Privacy Information Centers, "Privacy and Human Rights 2006–An International Survey of Privacy Laws and Developments" (EPIC 2006), http. www epic org. (Last accessed: 16 November, 2018).

[213] Report titled: "Cyberspace Policy Review-Assuring a Trusted and Resilient Information and Communications Infrastructure". (2009). Online available and retrieved from: https://www.energy.gov/cio/downloads/cyberspace-policy-review-assuring-trusted-and-resilient- information-and-communications (Last accessed: 20 November, 2018).

the standards of reliability of Critical Infrastructure Protection (CIP) through legislation "Title 16 – Conservation, Section 824o – Electric Reliability (16 U.S.C 824o)".[214]

Similarly, the flow of information is also secured by Federal Information Security Management Act 2002 (FISMA). On the other hand, ISO/IEC 27011, ISO/IEC 27002 and ISO/ IEC TR 27015 management guidelines are designed to secure ITs, information communication and information techniques in telecommunications and e-financial services. In addition to all these measures the Government also promoted the cybersecurity measures by making national level certification schemes.[215]

The US Legislative Measures Protecting Privacy from Government

Customarily, Americans have favoured the right "to be let alone" from their government. They prefer "life, liberty and pursuit of happiness"[216] as compared to the citizens of other states who demand "peace order and good government".[217] The advent of 9/11 has strengthened the belief that the privacy must be protected from Governmental institutions.[218] Americans' privacy is protected not only from government but also from the abuse of private sectors. This protection of privacy from government and private sectors is considered as liberty by the US citizens. In US privacy is considered as one's liberty and the protection of privacy is equal to the protection of liberty. In this head the US privacy legislation related to the collection and usage of personal data by government and private sectors is analyzed.

---

[214] Irion. "The Governance of Network and Information Security in the European Union: The European Public-Private Partnerships for Resilience (EP3R)." Springer Publ., (2012).

[215] Muazzam Mohamed, "Cyber Security Standards Compliance: A Vital Measure to Critical Infrastructure Protection", *KPMG*, (2015).

[216] United States Declaration of Independence (1776).

[217] Constitution Act UK, (1867).

[218] Marsha Cope Huie, Stephen F. Laribee & Stephen D. Hogan. "The Right to Privacy in Personal Data: The EU Prods the US and Controversy Continues" 9 *Tulsa Journal of Comparative & International Law* 391, (2002).

The Privacy Act of 1974[219] is the single legislation enacted by federal government to govern the informational privacy and to protect the data processed by the federal government. It is not applicable to the protection of such data which has been collected by state governments and private segments.[220] This Act also provides the provisions for federal agencies to collect the certain data for specified purposes and to maintain this data for such time as is appropriate for necessary actions. It also enables the individuals to review this data and to make any corrections or to update it accordingly. Moreover, it gives the opportunity to the federal agencies to protect this data and information from any abuse. It directs the federal agencies to collect and retain only relevant and desired information. This Act offers some exceptions to the federal agencies to transfer data and information among themselves under the blanket of "routine use exceptions" to justify such sharing of information.[221]

The Electronic Communications Privacy Act (ECPA) of 1986[222] bounds government officials to obtain the permission from a federal judge before receiving or interception of any electronic communication. The emails, internet service provider logs and public library pattern records are the examples of such electronic form of information and communication. This Act is aimed to protect the information and data which is generated, gathered and transferred by means of electronic communication frameworks.

---

[219] The Privacy Act of 1974, Available at https://www.justice.gov/opcl/privacy-act-1974. (Last accessed: 16 Nov, 2018).

[220] The implications of the tort of privacy on data protection have been limited.

[221] Chris Hoofnagle, "Big Brother's Little Helpers: How Choice Point and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement" 29 *North Carolina Journal of International Law & Commercial Regulation*, (2004).

[222] The Electronic Communications Privacy Act (ECPA) of 1986, https://search.justice.gov/search?query=The+Electronic+Communications+Privacy+Act+of+1986+&op=Search&affiliate=justice (Last accessed: 16 November, 2018).

The Privacy Protection Act of 1980[223] as compared to its title, this Act deals with the right and freedom of free speech. However, the right to privacy is also indirectly attach with this right to free speech. As this Act restrict the government to make any search and seizer of any work or material of a person who wants to publish such material in some kind of public communication. However, if any search or seizer of such material is inevitable than it can be done only after obtaining a judicial order.

The Family Educational Rights and Privacy Act (FERPA)[224] was adopted in 1974 to protect the records of students. The educational institutions such as universities and colleges are directed to protect the records of those students who are receiving any federal funding. The students' records cannot be shared to any other person without the consent of the said student. The institutions are also bound to provide the opportunity to the students to visit their records and to challenge any discrepancy. Students also have the right to update or amend any record related to them.[225]

The Driver's Privacy Protection Act[226] was passed in 1994. This Act provides the protection to the drivers' personal information. This Act forbids the motor vehicle departments of states to disclose the information of drivers for marketing purposes. Such information can be disclosed only after obtaining the consent of the individuals. However, this Act does not control the sharing of information without permission for toll tax payment and personal investigation purposes.

---

[223] The Privacy Protection Act of 1980, https://www.justice.gov/archives/jm/criminal-resource-manual-601-privacy-protection-act-1980 (Last accessed: 16 November, 2018).

[224] The Family Educational Rights and Privacy Act (FERPA),1974 https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html (Last accessed: 16 November, 2018).

[225] https://www2.ed.gov/policy/gen/guid/fpco/brochures/parents.html (Last accessed: 16 November, 2018).

[226] The Driver's Privacy Protection Act,1994 https://dor.mo.gov/media/dppa.php (Last accessed: 16 November, 2018).

The Right to Financial Privacy Act[227] provides the protection for financial records. These records are secured and made confidential from government and its agencies. The bank records of persons are specifically ensured and protected from any access and seizure by any government agencies in fourth amendment. Without the warrant of competent court such record cannot be accessed or detained. Moreover, the financial segments are also not permitted to obtain the blanket consent from their customers to disclose their data for unspecified business purposes. Customers also have opportunity to review and question their records.

The Fair Credit Reporting Act (FCRA)[228] was adopted in 1970 and amended in 1996 and again in 2003.[229] The main purpose of this Act is to maintain the accuracy of credit record of a consumer. It empowers the Federal Trade Commission to monitor the private sectors in credit reporting. The consumer reporting agencies are directed to report the exact and fair record of consumers without any errors. It is also demanded to report the dispute regarding any record of credit. It also provides strategies to measure the identity thefts.[230] Along with these provisions this Act also requires some privacy measures to be adopted by reporting agencies to keep the information of consumers protected from misuse.[231]

The Financial Modernization Act[232] was adopted in 1994. This act is pioneer to deal with the protection of privacy in financial domain. As compared to the Act FCRA, mentioned above, this

---

[227] The Right to Financial Privacy Act, 1978 https://www.federalreserve.gov/boarddocs/supmanual/cch/priv.pdf (Last accessed: 16 November, 2018). The Act was passed in response to *United States v. Miller*. 425 U.S. 435.

[228] The Fair Credit Reporting Act (FCRA), https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act (Last accessed: 16 November, 2018).

[229] This latest amendment is also known as the Fair and Accurate Credit Transactions Act (FACT Act).

[230] http://www.money-zine.com/Financial-Planning/Debt-Consolidation/Identity-Theft-Regulations/ (Last accessed: 16 November, 2018).

[231] The measures in the Act do not apply to information contained in credit reports that is available elsewhere, such as names and addresses.

[232] The Financial Modernization Act, 1999 https://www.investopedia.com/terms/f/financial-services-act-of-1999.asp (Last accessed: 16 November, 2018).

Act not only restricts the government institutions to share the information but also makes it compulsory for financial institutions to provide a privacy policy to customers for disclosure of information. This privacy policy must be shared with customers to make certain information available for business purposes. This Act is also governed by Federal Trade Commission (FTC).

The Identity Theft and Assumption Deterrence Act, 1998[233] is made to provide the remedy for victims whose identity is used by any other person for criminal purposes. This Act provides the punishments of fine and imprisonment for thieves of identity crimes. This Act does not discuss any provision of privacy but only addresses the relief after making the crime of using identity for illegal purpose.

The Cable Communications Policy Act, 1984[234] is related to regulations formulated for cable industry. The cable providing companies are not permitted to collect such information which is not specified in the Act. The cable companies are allowed only to gather the relevant information and this information is not collected without the consent of the customers. This Act also requires maintaining and protecting the privacy of information and prohibits the disclosure of such information to the third party. However, such information may be shared in case of any necessity to avail some services.

The Videotape Privacy Protection Act[235] is a milestone towards the privacy and protection of personal information in America. This Act was promulgated after the happening of an unwanted incident. A video related to rental records was released by Bork, a judge, which was against the

---

[233] The Identity Theft and Assumption Deterrence Act, 1998, https://www.ftc.gov/node/119459 (Last accessed: 16 November, 2018).

[234] The Cable Communications Policy Act,1984 https://www.govtrack.us/congress/bills/98/s66 (Last accessed: 16 November, 2018).

[235] The Videotape Privacy Protection Act, https://www.loc.gov/law/find/hearings/pdf/00183854811.pdf (Last accessed: 16 November, 2018).

privacy policy of the citizens as well as the profession of Judiciary. It was asserted in this Act that the video records of customers shall not be disclosed without their permission. Further, it also makes it compulsory to discard the record related to personal information within the span of one year. As such record is not required to be collected and retained for more than the time period of one year. This Act is directly related to the protection of privacy and personal information of individuals. It also prohibits the misuse of personal information and secure the data from such abuse.

The Telephone Consumer Protection Act, 1991[236] deals with the privacy of consumers to be let alone and not be interfered. The telemarketers are required to keep an updated list of such customers who do not allow themselves to be called for marketing purposes. This "Do-not-Call" list is also established by Federal Communication Commission to be provided to telemarketers. This Act specifically addresses the right to privacy by providing telemarketers the specified list for not calling certain customers and refrain them from interfering into those customers' privacy by letting them alone.

The Telecommunications Act of 1996[237] is also related to privacy of customers in telemarketing industry. But this Act is particularly designed for telephone companies to restrict them to track the call patterns of their customers. This Act is passed for customers privacy in their personal life and to make them free from any tracking by any telephone service providing companies. This Act is the updated form of the Communication Act, 1934.[238]

---

[236] The Telephone Consumer Protection Act, 1991 https://www.fcc.gov/document/telephone-consumer-protection-act-1991 (Last accessed: 16 November, 2018).

[237] The Telecommunications Act of 1996 https://www.fcc.gov/general/telecommunications-act-1996 (Last accessed: 16 November, 2018).

[238] http://www.fcc.gov/Reports/1934new.pdf (Last accessed: 16 November, 2018).

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[239] was designed to remove the "Job-Lock" that was in existence because of personal medical information of employees. This Act addresses some privacy concerns of individuals which shall not be disclosed to the employers. The personal medical information related to health issues, health services and health insurance plans cannot be transferred to any person without the consent of the patient. This consent must be obtained by express provisions and before any treatment. Such consent to the disclosure of any specific information must also bring into the knowledge of a patient. Further, the care providers are also under civil and criminal liability in case of any breach to the privacy of personal information of the patients. The patients have a right to access and review the information which they have allowed to be disclosed. This Act is administered by health department to keep the personal information of people protected and secured.

The Children's On-line Privacy Protection Act of 1998 (COPPA)[240] was adopted in 1998 to protect the information and privacy of children. This Act provides the regulations to the websites and online service providers to keep secure information gathered from children. It also directs the websites to contact the parents of the children who are at 12 years or below 12 years to contact with their parents for the gathering of any personal information. The parents should be kept well informed by these websites about every information accessed by children. Moreover, the parents also have the right to review and correct the information provided by their children. Similarly, some information may not be directly gathered from children.[241] In this way, this Act provides

[239] The Health Insurance Portability and Accountability Act of 1996 (HIPAA) https://www.hhs.gov/hipaa/for-professionals/index.html (Last accessed: 16 November, 2018).

[240] The Children's On-line Privacy Protection Act of 1998, (COPPA) http://ftc.gov/ogc/coppa.htm (Last accessed: 16 November, 2018).

[241] Report of Federal Trade Commission titled: "Protecting Children's Privacy under COPPA: A survey of Compliance", 2 April, (2002).

great safety measures from misuse of any personal information about children. Moreover, this Act is not the part of any other Acts which are related to children rights such as the child Pornography Prevention Act etc.

The Patriot Act was passed after the incidence of 9/11. After the advent of 9/11 the US congress adopted the USA Patriot Act to protect the attacks from terrorism. This Patriot Act amended the various Acts and allows the government to interfere with the privacy of individuals. This Act amended the provisions of ECPA in order to empower the government officials to read the addresses of electronic communications such as emails and the websites that have been visited and searched to prevent the transfer of any sensitive information.[242] However, the contents of email are exempted to be read in order to maintain the privacy of people.

The Patriot Act also amended the FEPRA and allowed government officials to access the data of students to track any terrorism activity.[243] Government can approach the record of information about students in good faith to control the anti-national practices. The information provided to public universities, colleges and libraries are in the access of government without any prior permission of court except upon the plea of doing any investigation. The libraries are bound to keep it secret that the record of any person has been demanded by government.[244]

---

[242] "The Act has effectively extended the "pen/trap" rule of *Smit*, to electronic communications. 442 U.S. 735 (1979) has been described by Simmons, as a troubling case. The Court held that electronic devices able to capture all phone calls made from a phone line. known as "pen/trap" devices were not a "search" under the Fourth Amendment as the individual had "voluntarily" turned information over to the phone company".

[243] Nancy Tribbensee. "Privacy and Security in Higher Education Computing Environments after the USA Patriot Act" 30 *Journal of College & University Law*, (2004): 337.

[244] Lee Strickland, Mary Minow & Tomas Lipinski. "Patriot in the Library: Management Approaches When Demands for Information Are Received from Law Enforcement and Intelligence Agents", 30 *Journal of College & University Law* 363, (2003).

The US Constitutional Concerns and the Right to Privacy:

The constitution of the US does not contain any express provision of privacy. The bill of rights, however; is present there to express the intentions of framers to protect the privacy of peoples. First amendment is related to the privacy of one's beliefs. The third amendment protects the privacy of home of a solider. Fourth amendment provides the privacy to a person and possessions from unlawful seizer and searches. This amendment ensures that the persons, their houses and their papers are secure from illegal and unjustified searches and confiscations without a warrant but upon lawful reasons only. Fifth Amendment gives the right to privacy to personal information against self-incrimination. 19th amendment was adopted to protect the privacy of individuals in general sense. This amendment protects the rights related to privacy which have not been addressed in first eight amendments. It further explained that a right that is not implanted in constitution is not meant that it will be infringed, denied and kept unprotected. Later in fourteenth Amendment the right to privacy was favoured in the cover of right to liberty.

The Supreme Court of the US, endorsed the right to privacy in its various judgments. In *Griswold V. Connecticut*, Supreme Court struck down a state legislation related to the prohibition on the use of contraceptive and birth control pills for married couples. Similarly, in *Roe v. Wade*[245] case, the Supreme Court again recognized the right to privacy by acknowledging the women's right to have an abortion. Further, in *Lawrence v. Texas,* the court endorsed the right to privacy in relation to sexual practices of same sex couples.

[245] *Roe v Wade* (1972) 410 U.S. 113.

The US Response to the Privacy Directive: The Safe Harbor Agreement[246]:

The EU Privacy Directive empowers the EU Commission to restrict the transfer of data to the third countries if it is of the opinion that the third countries are not observing and obeying the adequate standards of data privacy. The safe harbor agreement ensures the EU that the US companies will follow the adequate level of data privacy regulations to protect the data transferred to these US companies. This agreement further allows EU to receive the data of the US only upon such terms and conditions which are sufficient for the protection of privacy of its citizens.

This agreement also deals with the data privacy protection of US Safe Harbor privacy regulations. It is also worth mentioning that this agreement is mainly related to the privacy of EU citizens. While it deals little with the protection and privacy of data of Americans. This agreement provides the seven basic principles for the protection of data that is transferred to the third countries for business purposes. These principles are the reflection of the regulations designed by OECD, the EU convention and Privacy Directive. These principles of safe harbor are related to the notice, choice, collection, transfer, security, integrity and enforcement of data privacy measures. The desired companies and business industries certify themselves as the privacy abiding entities so that the business may be carried on with them. Sometimes these companies may make contracts to the EU directly to do a business with each other.[247]

---

[246] EC, Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament, O.J. L. 215/007, (2000).

[247] Art. 26 of the EU Privacy Directive, (1995). This Article "offers the use of these clauses to firms for individual business transactions as an alternative to conformance with the Safe Harbor provision as outlined in art. 25".

Argentina:

The constitution of Argentina gives the right to privacy to the citizens in its Article 19. This Article provides that the conduct of the people which does not infringe the public peace and security nor damage the morality or harm the third party shall not be questioned by the jurisdiction of a court. As this conduct is related only to the affairs of God.[248] It further gives the right to its citizen by letting them free to do what is not restricted by law and not to compel them for doing a such thing which is forbidden by law.

Similarly, the Article 43 of the constitution gives the right to habeas data. It states that a person may demand to acquire information about any data which is attributed to him available in public records or data basis. Moreover, if he finds that the information is false, he may demand the rectification, removal or update of the said data. It also provides the opportunity for suppression or secrecy of such data which is discriminatory in its nature. The right to privacy is also protected under civil code at article 1071 bis.[249] The court may cease any activity which amounts a threat to privacy of any person or it may award damages if any loss has been done to the privacy of a person. In many cases the court issued injunctions against search engines regulated by Google and Yahoo.[250]

Argentina Penal code also makes it a crime to violate the electronic communications norms. Article 153 makes it punishable if someone gains unauthorized access to one's computer or changes any

---

[248] Decided on 11 December 1984, Corte Suprema de Justicia de la Nacion (CS), para. 8.

[249] Added by Article 1 of Law N 21.173 and published in the Official Gazette on 22 October, (1975).

[250] Much of the information about these cases comes from E. Compa and E. Bertoni, "Emerging Patterns in Internet Freedom of Expression: Comparative Research Findings in Argentina and Abroad" (Centro de Estudios en Libertad de Expresion y Acceso a la Informacion (CELE)). Online available at: http://www.palermo.edu/cele/libertad-de-expresion-en-Internet.pdf. (Last accessed: 16 Nov, 2018).

data or alters any information or steal any data from computer.[251] It is also a crime if someone obtains the access unlawfully to other person's personal communications, emails, letters, telegraphs or faxes. The Argentina is the first country in Latin America which has adopted the measures of European Commission to secure the free flow of data and to make the communications safe in business. The Personal Data Protection Act, 2000[252] is also drafted by Argentina to make the electronic communications protected and to give a shield to personal data.

Canada:

There are no clear provisions of right to privacy in the Constitution of Canada and Charter of Rights and Freedoms. While giving interpretation to the Section 08 of the charter, the Canadian Courts have acknowledged the right to privacy of a person. In section 08 of the Charter, the unnecessary searches and seizers are prohibited. It is stated that a person cannot be searched without reasonable grounds. The privacy has been also recognized in federal and provincial domains.[253]

Federal Privacy Act, 1982 was designed at federal level to secure the information and data of the citizens of Canada. Similarly, another Act was drafted to protect the personal information. This Act is known as Personal Information and Electronic Documents Act (PIPEDA) 2001.[254] These both Acts manage the flow of information collected by certain agencies. Further, they also provide the access to information and to update or amend such information which has been collected by such agencies. These Acts also give an opportunity to individuals to knock the door of the court if

---

[251] Published in the Official Gazette on 25 June, (2008).
[252] It was promulgated on 30 October, (2000).
[253] David Flaherty, *Protecting privacy in surveillance societies: The federal republic of Germany, Sweden, France, Canada, and the United States*, Chapel Hill, The University of North Carolina Press, United States, (1989).
[254] Personal Information and Electronic Documents Act (PIPEDA), 2001.

such information is refused to be accessed. However, the records of courts cannot be viewed. Similarly, it is also forbidden to make any question against the collection, usage or transfer of such information by any federal public agencies.

There are certain grey areas in the privacy laws of Canada. In this regard, the Privacy Commission, reviewed the privacy legislation. It finished its review in 1999 and offered one hundred suggestions to improve and amend the privacy laws. It was also suggested that the Commission should have the powers to collect and disclose the information. Further, the Federal Government shall also be directed by the Commission to collect, review or transfer certain information. Moreover, the courts will also be empowered to review information in a large scale. The rule regarding the collection, control and matching of information and data shall also be advanced. Restrictions shall be imposed on publicly accessible information.

Many reports are there in which the privacy breaches of Canada are stated. In February 2003, some cases of privacy breach were noticed. In these cases, the record of patients was disclosed on the backside of real estate's documents. It was reported that this record was provided to a law firm. This law firm used these papers as a recycling procedure of sheets. The Ontario Privacy Commissioner punished the law firm for mishandling of records. Similarly, a computer hard drive was also informed to be stolen. In this drive there was a record of thousands of customers of an insurance company. This recode was consisted of many valuable credentials including accounts statements, medical records and tax paying information. This incidence was a breach to privacy of customers records. The hard drive was found after a week because of making certain actions. But

it could not be assessed that how much data has been used. The personal information was not secure by any measure and it was quite easy to transfer it in other system.[255]

In June 2003, the computers were shut down in British Columbia at Courts. It was alleged that the record of court cases was in danger. A person was there in the courthouse building who could access information on such computers. To save the information the computers were kept close for many days. The privacy concerns are very critical in Canada. Many efforts are made by Government to control the privacy issues. Media has also played very important role in this regard. Alberta Information and Privacy Commission submitted a report in which it was stated that public is not aware of privacy laws. Moreover, many people are not conscious about their personal information and its protection or secrecy.

3.3 Cyberspace Laws in Australia

In Australia the Federal Privacy Act, 1988[256] is there to deal with the matters related to the privacy of citizens. This Act is applicable to the Government, Australian capital agencies and some private organizations to handle the information of the people. This Act also regulates the process for collection, retention, usage, applicability and transfer of the information and private data. A Privacy Commission is also established under this Act. The privacy complaints are handled by the Privacy Commissioner. Some states of Australia have also made their own laws to deal with the privacy issues.

---

[255] Avner Levin and Mary Jo Nicholson, "Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground", *UOLTJ*, 2:2 357, (2005).

[256] http://www.oispp.ca.gov/consumer_privacy/default.asp> (Last accessed: 16 Nov, 2018).

The development of digital technology also encouraged Australia to develop its cyber security strategy. It was designed in 2009. This strategy highlighted the need to make a policy and standards for security of cyberspace. In this regard Protective Security Policy Framework (PSPF) is adopted along with ISO/ IEC AS/NZ 27001, which has 33 mandatory requirements to protect the government's people, information and assets.

In addition to these standards, the American National Standard Institute/International Society of Automation (ANSI/ISA)-99, Industrial Automation and Control Systems Security and ISO27799 Health Informatics - Information security management in health using ISO/IEC 27002 are also implemented voluntarily to prevent privacy intrusions and to protect critical infrastructure.[257]

3.4 Cyberspace Laws in European Countries

The examples of certain European countries are as follows:

France:

France has strong legal protection of privacy in its legal framework. The notion of privacy was adopted in France legal system after the advent of Strauss-Kahn affair. It was deemed that the rich and famous people were prevented to become the part of media acquaintance which had also benefitted the Strauss-Kahn's immoral acts to be remained covered.[258]

Further, the constitution of France offers the protection of privacy as it was asserted by the constitutional court of France in 1995[259] and 1999 respectively. France has also a Data

[257] Australian Government Report on "Cyber Security Strategy", (2009).

[258] David Flaherty, *Protecting privacy in surveillance societies: The federal republic of Germany, Sweden, France, Canada, and the United States*, Chapel Hill, The University of North Carolina Press, United States, (1989).

[259] http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les/decisions/acces-par-date/decisions-depuis-1959/1995/94-352-dc/decision-n-94-352-dc-du-18-janvier-1995.10612.html. (Last accessed: 16 Nov, 2018).

Protection Act, 1978[260] to maintain the privacy of personal data. This Act was amended in the light of EU Data Protection Directives[261] to provide a harmony with these Directives. It is also worth mentioning that the provisions of the Act require to expose the purpose for the collection of any information. It also directs the official to specify the time for the retention of any data and information. France has also adopted the Cookies Directive[262] which will inform the users before any installation or use of such cookies to protect the computers from any pirated software.

Germany

Germany is one of those countries which provides the strong and strict protection of data to is citizens. Germany introduced the data protection laws and right to privacy in early times as compared to other countries. Germany enacted its first legal draft addressing the right to privacy and data protection in 1970 on the Land of Hesse. The constitution of Germany also provides the right to privacy in Article 1 and 2 respectively. The citizens' dignity and privacy are made inviolable from unlawful intrusion and interferences. Germany has also adopted data privacy laws in the form of Federal Data protection Act, 1977 to make information secure in business spheres. The corporations are bound to protect the information and data of citizens from all type abuse. It also directs the specific purposes for which the information may be collected. The Act also restricts the tenure of retention of a specific data. In cooperation with EU the Germany has designed its regulations to control the flow of data to third parties. It has also rectified the EU Directive to

[260] Act n° 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties, as amended by Act n° 2004-801 of 6 August 2004 relating to the protection of individuals with regard to the processing of personal data.

[261] News Wires, Internet giants challenge French data law over privacy, 6 April, (2011).Online available and retrieved from: http: www.france24.com en 20110406-internet-giants-challenge-france-data-law-privacy-googlefacebook.- (Last accessed: 16 Nov, 2018).

[262] http. www.privacysecuritysource com 2011 09 09 france-implements-the-cookies-directiveand- (Last accessed: 16 Nov, 2018).

control the transborder flow of data to third countries. Germany has a set of certain provisions before sharing the information with third countries which are not the member of the EU. A Federal Data Protection Commission is established to monitor the flow of information and data as well as to enforce the data protection regulations.[263]

To safe the privacy of children Germany has acted as pioneer. It has many provisions to control the flow of data from children. It has restricted many companies to make such toys which are connected to networks or wifi, like "My friend Cayla". The children privacy is regulated by federal network agency known as Bundessnetzagentur.[264]

United Kingdom (UK)

The UK government has recognized the inevitable dependency upon digital technology as it has accessed that these technologies are a part of its economy and growth.[265] In 2010 UK did a largest internet-based economy of worth about USD188 billion.[266] Because of this reliance and dependency upon internet technology UK designed its cyber security strategy and its notion is "to derive huge economic and social value from a vibrant, resilient and secure cyberspace, it is vital that the country's basic infrastructure be protected".[267]

The UK government has designed cybersecurity strategy in the form of Minimum Security Standards (ND 1643), Network Interoperability Consultative Committee (NICC) and Communication Act.2003. To minimize the vulnerabilities in the country's government systems

---

[263] DD Hirsch, "The law and policy of online privacy: Regulation, self-regulation or co-regulation?", 34 *Seattle University Law Review*, (2011): 451.

[264] David Flaherty, *Protecting privacy in surveillance societies: The federal republic of Germany, Sweden, France, Canada, and the United States*, Chapel Hill, The University of North Carolina Press, United States, (1989).

[265] BBC, "UK is the 'most Internet-based major economy'", 19 March, (2012).

[266] Conversion rates taken from Oanda as on 31 December 2014: US$/ GBP 0.64374.

[267] HM Government, "The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world", November 2011.

and critical infrastructure UK has developed the cyber security and information assurance standards by designing Information Assurance Maturity Model (IAMM). To create a secure network IAMM is aligned to Security Policy Framework (SPF), ISO/IEC 27001 and the Business Continuity Management (BCM) standards (BS 25999/ISO 22301). The application and implementation of standards is encouraged by Government through the national-level certification schemes.[268]

3.5 Cyberspace Laws in Asia

The cyberspace laws of certain Asian counties are as follows:

China

The Government of China does not provide a wide range of privacy to its national. On the contrast the Chinese authorities and officials maintain a significant switch over internet and individuals' right to privacy. However, this trend is going to be changed because of undesirable intrusions into individual's life and privacy. Such as most of the private companies and business sectors invoke the unwanted interference into personal information specially the banks and motor vehicle companies which resulted into the amendments in criminal law and the law of torts. It also raised the new proposals towards the protection and privacy of data.

Article 40 of the Chinese constitution safeguards the privacy of an individual's correspondence from interference of any organization or person. No one is allowed to damage or attack the privacy of correspondence of an individual except with the due process of law or under the blanket of national security or public interest or any investigation.[269] Similarly, Article 38 of

[268] Muazzam Mohamed. "Cyber Security Standards Compliance: A Vital Measure to Critical Infrastructure Protection", *KPMG*, (2015).

[269] http://www.npc.gov.cn/englishnpc/Constitution/node_2825.htm. (Last accessed: 16 November, 2018).

the Chinese constitution addresses the personal dignity of an individual by forbidding the insult, libel, false accusation or wrongful incrimination. Moreover, Article 101 of General Principles of Civil law provides the remedy against the breach of reputation and protection of privacy.[270] The right to privacy is also protected by the seventh amendment in Criminal law.[271] This amendment is important as it provides the first independent action in case of breach of privacy. This amendment makes it punishable if any official of any organization, institution or public body including financial, medical or educational institutions sells or transfer the data and information of any person. Such organization's directors and employee shall be liable to pay fine and to imprisonment. This amendment is also significant as it also punishes the person who wrongfully or unlawfully gains any information.

Another advance step is also taken to protect the privacy by adopting Tort Liability Law, 2009. This law gives the remedy of damages if someone's privacy has been injured by unlawful means which resulted in emotional harm. Under this law, a medical officer may be held liable for breach of privacy if he discloses the information of his patient's health without his consent.[272] Another development has been made in the domain of privacy by adopting the Information Security Technology Guidelines for Personal Information Protection. These Guidelines are formulated by Ministry of Industry and Information Technology (MIIT), Standardization Administration of China (SAC) and the General Administration for the protection and security of information and data.

---

[270] Adopted on 12 April 1986. Available at: http: en.chinacourt.org public detail.php?id=2696. (Last accessed: 16 November, 2018).

[271] McKenzie and Milner, "Recent Developments in Data Protection", China Update, 9 March, (2009).

[272] Online available at: http: www.hunton.com files (Last accessed: 16 November, 2018).

The Guidelines provides the rules for collection, transfer and inspection of data. The computer processed data shall be collected only for specified purposes. It also restricts the collection of only relevant data. Further the Guidelines direct that the information and data collected from children below the age of 16 must be received by their parents. These Guidelines also provide the time frame for the retention of computer processed data. It further gives the provisions for the transfer of such data to third parties. Moreover, the transfer of the data to other countries is under more restrictions that have been designed by states themselves. These guidelines are also rigid for the cross-border flow of data.

Various sectors are also made safe for the protection and safety of information and data. Like the records of medical sector, educational sector, banking and credit sectors are made more secure by adopting legislations. The record and data related to computer systems at local level are also safeguarded by authorities for consumer protection.[273]

South Korea

South Korea is one of the most hyper-connected countries in the world.[274] South Korea is also among of those countries which have recognized the importance of cyber security. Because of its interaction with other nations through information technologies, it is the demand of hour to keep a safe and secure virtual world. According to the report of the Ministry of Strategy and Finance, there is a "high risk of intrusion into Korea's main national information communication infrastructures caused by cyberattacks". Network communications are made safe by making

[273] G. Greenleaf, "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention". *University of New South Wales Faculty of Law Research Series*, paper 42, (2011).
[274] J.M. Victor, "The EU General Data Protection Regulation: Toward a property regime for protecting data Privacy", 123 *The Yale Law Journal*, (2013): 513.

compliance with ISO/IEC 27001 and adopting the law, Act on Promotion of Information and Communications Network Utilization and Information Protection 2005 to make the privacy of user's personal information and communications.[275]

Japan

Like other vigilant and developed nations, Japan has also its strategy to protect its cyber domain. Like USA, Japan has also made much successful efforts to design cyber policies to secure its citizens in digital world. It started to design its policy regarding internet communication technologies in 2004. In April, 2005 Japan established its National Information and Security Centre (NISC) under the supervision of Government to monitor virtual information and activities in cyberspace. The NISC is also responsible for making information security strategies and to manage emergency situations to prevent damage to the information and data. In 2013 Japan founded its final cyber security strategy by designing various standards related to information technologies and security of cyberspace. It also provides the room to establish cooperation with private companies to protect critical infrastructure and to build interdepartmental relation by adopting the public-private partnership standards. Japan also took initiatives to develop an international cybersecurity.[276]

India

The constitution of India does not explicitly talk about the right to privacy. However, Article 21 of the Indian constitution deals with the right to life which is interpreted by the supreme court of

[275] Report of Ministry of Strategy and Finance, "2011 Modularization of Korea's Development Experience: Information Security Activities in Korea". (2012).

[276] Kyoung-Sik Min, Seung-Woan Chai and Mijeong Han, "An International Comparative Study on Cyber Security Strategy", *International Journal of Security and Its Applications*, Vol.9, No.2 (2015): 13-20.

India that the right to privacy is also embedded in the right of life. It is asserted by the Supreme Court that right to life also includes the right "to be left alone". The privacy of the citizens must be safeguarded. A privacy of a person also includes the privacy of his family, home, marriage, procreation of children, educational and medical records as well. No one is allowed to infringe the privacy of a person or to make interference with it. If someone infringes the privacy of other person, he will be liable to pay damages.[277]

The Indian Telegraph Act, 1885[278] and Information Technology Act, 2000 regulate the telecommunications and protect them from any intrusion or breach of privacy.[279] These Acts also protect the national integrity and security of India as well as provide the regulations for friendly relations with other countries. The Telecommunication Regulatory Authority of India was established by Telecommunications Regulatory Authority of India Act, 1997. This authority has made many orders to shield the privacy in the telecommunication domain. The Right to Information Act, 2005 is also present in Indian legal framework to protect the information by excluding the access of public authorities to certain information of private nature related to an individual which does not amount as public information.

On April 2011, the Indian Ministry of Communications and Information Technology has also adopted certain Information Technology rules 2011, under the influence of Information Technology Act, 2000 which was amended in 2008[280] to secure data in telecommunications. The

---

[277] *R. Rajagopal v. State of Tamil Nadu* (1994) 6 SCC 632. This case extended the right of privacy by placing an obligation on the State to prevent private intrusions. The right was first recognized by the Supreme Court in *Govind v. State of Madhya Pradesh & Anr* (1975), SCR (3) 946.

[278] Sections 5 and 7 of the Indian Telegraph Act, (1885).

[279] Ibid; Section 66-E.

[280] section 34, amending section 69 of the original act and introducing new sections 69A and 69B of the Information Technology (Amendment) Act, (2008).

Telecommunications Regulatory Authority of India (TRAI), developed by the Telecommunications Regulatory Authority of India Act, 1997, follows certain rules before proceeding with the data. These rules require the consent of the subject before the collection, retention or transfer of any data.[281] These rules also direct to use the data only for desired purposes.

3.6 Emergence of Data Protection in Cyberspace Technology

The interest to protect the data and information in cyberspace developed in 1970s. The advanced technologies and devices expanded the needs to draft legal framework for managing private information and data. Large number of nations acknowledge this right to privacy in their legal structure. In 1970, Germany adopted its first enactment regarding the protection of data and information in cyberspace. This right of data privacy was endorsed by Sweden legislatures in 1973. The US had also adopted this right in 1974 and France added this right in its legal framework in 1978.

Two important international instruments got birth from this trend-to protect data and information-in order to maintain privacy in digital world. First enactment is the "Council of Europe's (COE) Convention 1981 and the second is "Organization for Economic Cooperation and Development's (OECD) Guidelines" for the Protection of Individuals with regard to the "Automatic Processing of Personal Data". These instruments explicitly deal with the rules for governing of the Protection of Privacy and Transborder Data Flows of Personal Data and also introduced standers for protection of data and privacy. It is also pertinent to mention that the guidelines inside these two records shaped the spirit of the Data Protection laws of many nations. As these principles depict the individual's data and information as key rights which are to be

[281] *People's Union for Civil Liberties (PUCL) v Union of India and Anr.* (1997) 1 SCC 301.

secured at each step of gathering and dispersal. In these instruments the interest of individuals to approach and alter their information is affirmed as a primary right and therefore made an essential part of these principles. More than twenty nations have embraced the COE Convention and another six have marked it however have not yet received it into law.[282] The OECD rules have likewise been generally utilized in national enactment, even outside the OECD nations.

The idea of data privacy, in different documents and legal frameworks, changes just by degrees. All documents necessitate that the individual's information and data must be acquired reasonably and legally, used only for defined purposes, proper and sufficient for the desired cause and discarded after its motivation and task is finished or accomplished. These two declarations have profoundly affected the reception of laws around the globe.

Privacy was addressed first time in the US by Samuel Warren and Louis Brandeis in their article.[283] This article was written to highlight the increment in daily papers and photos made conceivable by printing advancements. Advancement in technology has made it easy to collect sensitive information and data. Similarly, warmth sensors were expected adequate to be utilized to discover cannabis (marijuana) developing activities. In 2001 in *Kyllo v. United States*[284], it was held that the thermal imaging gadgets that can uncover past obscure data without a warrant is undoubtedly constitute an infringement of privacy.[285]

---

[282] Patrick, P. Howard. "Privacy restrictions on transnational data flows: a comparison of the council of Europe draft convention and OECD guidelines." *Jurimetrics* 21, no. 4 (1981): 405-420.

[283] Samuel Warren and Louis Brandeis, "The Right to Privacy", *Harvard L.R.* 193 (1890).
[284] 533 U.S. 27
[285] http://plato.stanford.edu/entries/privacy/> (Last accessed: 20 November, 2018).

By and large, the expended capacity to collect, retain and forward data had developed negative approaches to breach privacy. Computer networks and advanced frameworks become so typical that they had made it possible to retain a large number of data and information on database at huge scale. A person is unable to know or to manage the large part of data about him which other persons may approach. Such data and information are sold to other persons for some benefits without the knowledge of the person to whom this data is belonged. The sense of data privacy has become more important as more networks are going to collect and manage more data. Consequently, the breach of privacy may be resulted more serious. In various countries there is a great need that privacy related laws are to be amended to make technologies more secure and safe to keep up individual's right to privacy. The current worldwide system of privacy right is considered insufficient and muddled.

Apart from these dimensions of privacy, there are also some other numerous elements which are responsible for intrusions into one's security and privacy i.e. Globalization, Convergence and Multimedia. Globalization evacuated the land constraints to the stream of information. The improvement of the Internet is the best-known case of a worldwide innovation. Convergence, lead to the ablution of obstructions between advance technologies and frameworks to trade and process diverse types of information. On the other hand, Multimedia, combined numerous types of transmission and articulation of information so that data accumulated in a specific shape can be effortlessly converted into different structures.[286]

[286] A.B. Makulilo, "Myth and reality of harmonisation of data privacy policies in Africa", 31 *Computer Law & Security Review*, (2015): 79.

As the advancement in technology introduced the new crimes. Data privacy is also a concern for many nations with the evolution of internet and other computer-based networks. Personal information has become more vulnerable in the digital era. Individual's data needs more security measures at international level because of the transborder nature of the technology. Information technology is not limited to the borders of any state. It shares the data and information on a global network which may be accessed from any part of the world.[287]

A single click on mouse can intervene into the computer of any person which is located in any part of the globe. In this regard many nations have tried to secure the information in cyberspace. International Organizations are trying to combat the cybercrimes. They are modifying and updating their regulations to address this dimension of data privacy. The OECD, the council of Europe, the EU, the G8, the APEC and Interpol are the illustrations of such organizations which are endeavouring to make such rule which may be beneficial for member states to secure the information and data of their citizens. It is also necessary to develop such laws which may help to make offenders punishable for such transborder crimes. The right to privacy has also been acknowledged by many countries. At national level several states have been introduced the right to privacy in their constitutions and legal systems. International instruments surely performed a great role in this regard. Like, OECD guidelines, EU Data Privacy Directive and the COE Convention encouraged the countries to make laws relevant to the protection of privacy at national level.

[287] The title of the OECD data privacy instrument is: "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data."

3.5.1: Privacy Regulations adopted by European Organizations

Europe has made many efforts to protect the personal information and private data of individuals. It is considered as a leader to make laws and regulations for the privacy of information and data in various sectors of the transactions. Moreover, it has set a trend to protect the rights of individuals related to information and data protection in commercial milieu as well. It is also a step forward from US and other countries in data privacy domain by making a number of practices illegal associated with compilation and exchange of information and data.[288]

Similarly, it also provides a complete guideline for the business segments to transfer data and information with other countries on settled principles. It is the opinion of some experts that the US will consider European provisions of data privacy as a fit rule for data security of its individuals especially in commercial era.[289] Europe has also endorsed the protection of privacy as a human right in the Convention for the Protection of Human Rights and Fundamental Freedoms.[290]

The Organization for Economic Cooperation and Development (OECD), 1980

International streams of information and data woke the necessity of a universal legislation so that a legal framework may be there to control the difficulties arising out from such proliferation of data. This flow of information made the transactions and business more complicated for

---

[288]Avner Levin and Mary Jo Nicholson, "Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground", *UOLTJ*, 2:2 357, (2005).

[289]" Directive 95/46/EC of the EU has forced the US government to consider the invasiveness of currently accepted business practice and to enact ameliorative law, then American society, in particular the consumer who alone pitted against business's short-term interests carries little political weight, owes much to the European privacy impetus. It would benefit global society to adopt the philosophy of the directive as the new *ius gentium* for data- privacy law."

[290] Art. 8 of the ECHR assert that: "the right to respect for private and family life".

international trade community.[291] OECD is an international organization which stepped forward to make regulations for the protection and security of information.[292]

In 1981, the OECD adopted its Guidelines on the protection of personal privacy and transborder flows of personal data. It was the first agreement dealing with transborder flow of information and its protection. The important thing is this at the time of framing these Guidelines the Council of Europe was also taking initiatives to protect the data and information. Thus, the corresponding organs of the Council of Europe were kept in contact so that these rules may not become contradict to the policies of those organs.[293] In this way the language of principles is adopted in parallel senses by both organizations.[294] It may be said that these Guidelines mirror the principles established by the Council of Europe in its convention. The Guidelines are anticipated to make rules related to privacy of information and data at national and international level. Eight basic principles are introduced for the collection, gathering, retaining and securing of data for lawful purposes. Further, these Guidelines also addresses the limitations for data collection, liability of data collectors, individuals right to access the data and openness of data for legitimate and specified objects.

The Guidelines are not binding on member states. The member states are at liberty whether to follow these guidelines or to frame domestic legislations in accordance to these principles. The guidelines are so flexible as they are easily capable of being adoption in the legislation of a state

---

[291] Paul M. Schwartz, "Preemption and Privacy", 118 *YALE L. J.* 913 (2009).

[292] Colin J. Bennett & Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, 88, MIT Press, 2d ed. (2006).

[293] For instance, "whether data privacy referred only to automated processing or how sensitive data should be processed", OECD, art. 4 and Explanatory Memorandum.

[294] Michael Kirby, "The History, Achievement, and Future of the 1980 OECD Guidelines on Privacy, Address at the Round Table on the 30th Anniversary of the OECD Guidelines on Privacy", in Paris, France (10 March, 2010): 136.

instead of taking the whole guidelines in national legal framework.[295] The major emphasis is given to the free flow of information and to control hurdles in making any transaction of business. Its aim is to promote the international cooperation in economic and social sectors of member states rather than to formulate uniform pattern of legislation. It also wilfully refrained from partnership in disputes arising from the flow of information.

Moreover, the OECD intended to furnish the general and broad consensus of member states in such a way as to build common principles to boost cooperation among them. However, these Guidelines become more significant and effective after the adoption of EU directives seventeen years later. Because of this flexibility and diversity, the member states i.e. UK, USA, Canada, Germany, Japan and Korea had adopted these guidelines for the protection of data.

The Council of Europe's Data Privacy Convention, 1981

The Council of Europe was established in 1949 after the advent of World War II. The council talked about the problem of privacy and protection of personal data in the very year of 1949. These efforts continued for a long time. With the advancement of technology, the council started its work in 1968 to cater the privacy issues of personal information and data generated by ICTs.[296] In 1981, the Council of Europe held its convention 108 regarding the protection of Automatic Processing of Personal Data of individuals.[297] The Convention provides the measures to protect the personal information of people. It also set out a data privacy model for those countries which don't have laws on protection of privacy.[298]

---

[295] Ibid;

[296] "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data", Explanatory Report, Jan. 28, (1981), E.T.S. 108.

[297] Ibid;

[298] Ibid;

The convention demands certain formalities for the protection and security of atomically processed personal data. In this regard the convention stresses upon firm principles. Such as the data must be gathered and processed lawfully. It should be used for specified and legitimate purposes only. The data should not be collected and retained for unlawful or incompatible aims. The data must be relevant and limited to the specified object. The data should be gathered into such limit only as it is prescribed for the definite purpose. It should keep up to date and for required time only. The data should be protected and secured from any interruptions. The convention also provides the right of access to individuals to check the genuineness of such data and to make any corrections of it if it is needed.

This convention is considered as a milestone for further legislation on data privacy measures in Europe and other countries. This was the same time when OECD was also formulating its guidelines for protection of transborder flows of data and personal privacy. However, unlike the OECD the convention is the sole international legal framework which requires its signatory states to adopt its principles in their domestic legislation. It is bifurcated into various sections related to the privacy rights of individuals and the protection of data.[299] It also bounds the member states to harmonize their domestic laws with these principles. It also directs the member states to consult with each other and to keep themselves updated in the matters of information technology. It is also suggested that the states should enhance the international cooperation by keeping themselves aware with the issues of data security.[300]

---

[299] Paul de Hert and Eric Schreuders, "The Relevance of Convention 108", Paper presented at "the European Conference on Data Protection on Council of Europe Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data: Present and Future", in Warsaw, 34 (2001).

[300] "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data", Jan. 28, (1981), Explanatory Report, para. 11.

The convention introduces a bilateral mechanism among member states to handle the disputes and matters of data privacy rather than formulating the international organization to manage these concerns.[301] It is also remarkable that it is the first convention which set a criterion for flow of personal information between two states. It allows the state to transfer the data of its individuals to the other state upon the condition that the both states should have laws on adequacy criteria for data exchange. It restricts the national powers and officials of a state to exchange the personal data of individuals with those states which do not have enough legislation on adequacy criterion for such transfer of data.[302] The Council also kept cooperation with the OECD during the adoption of this convention[303] which resulted into the uniform principles for cross-border streams of data. Along with the OECD, the Council also added the Japan, USA, Canada and Australia as the observers of convention.[304]

The European Telecommunications Directive and the European Data Protection Directive:

The European Union (EU) had drafted two mandates which furnish individuals with a more extensive scope of insurances over misuse of their information. The Directives provide a gauge for normal level of security which strengthens current information insurance law, as well as which extends it to build up a scope of new rights. The Data Protection Directive forwards a standard for domestic law which will tone the law for entire EU". According to these directives each state of EU must had to pass harmonizing enactments by October 1998, however it is more probable that not all had finished the procedure until the early of 1999s. The Telecommunications Directive built

[301] Among which the most notable example is the United Kingdom, followed by the Netherlands, Australia and Japan.
[302] Article 12 of the Convention 108, Council of Europe.
[303] Colin J. Bennett & Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, 88, MIT Press. 2d ed. (2006).
[304] Ibid;

up particular assurances related to phone, advanced television, mobile systems and different media communications frameworks.[305]

A few standards of information assurance are protected under the Directives, to be specific the right to know from where the information generated, the right to amend the incorrect information, a right to take action in case of unlawful handling with data and the right to consent to utilize information in a few conditions. For instance, people will have the right to make options to forward material without giving a particular reason and without any cost. The Data Protection Directive contains securities over the utilization of individual information relating to wellbeing, medical care or financial matters. In future, the business and government utilization of such data will by and large require "unequivocal and unambiguous" assent of the information subject.[306]

The basic idea in the European model is "enforceability." The EU emphasized that "information's subjects have rights that are incorporated in express guidelines. These guidelines may address an individual or an expert who can follow up for their sake". Each EU nation is required to establish a "Privacy Commissioner or organization to implement the standards. It may happen that the nations with which Europe works together should have a comparative level of oversight".[307]

The Directive levies a commitment on member nations to guarantee that the individual's data dealing with European subjects must be secured by law when it is shared with nations outside the

---

[305] Bhaimia, Sahar. "The general data protection regulation: the next generation of EU data protection." *Legal Information Management* 18, no. 1 (2018): 21.

[306] L Bergkamp. "The privacy fallacy: Adverse effects of Europe's data protection policy in an information-driven economy", 18(1) *Computer law & Security Report,* (2002): 31-47.

[307] M.D. Birnhack, "The EU Data Protection Directive: An engine of a global regime", 24(6) *Computer Law & Security Report,* (2008): 509.

Europe. This necessity has brought about requirement to draft privacy laws outside Europe for the protection of data. Those nations which have declined to receive significant security law may get themselves unfit to direct certain kinds of data rules to harmonize with Europe especially in the case when they include delicate information.

The Telecommunications Directive demands a wide range of responsibilities from experts and service providers to protect the data of customers and to maintain the privacy of users. The new guidelines and rules address those angles which have gotten lost in an outright flood of information and data protection laws. Approach to billing information is made extremely limited. Caller ID technologies must be kept restricted to a limited transmission. Data which is collected from the transmission of a communication must be discarded after the call.[308]

The European Union's Data Protection Directives, 1995

The European Union started its work on data privacy in 1995, that become prominent at regional as well as International level. Its important document on privacy is European Union's Data Protection Directive[309] which became effective in 1998. The major object of EU Data Protection Directive was not only limited to the protection and privacy of data but also to provide the trade liberalization. It was also aimed that a sole integrated market may be attained as it is suggested by the EU policy.[310]

This Directive deals with the processing of all forms of Data. It also provides the exceptions

---

[308] O Lynskey. "Deconstructing data protection: the 'Added-value' of a right to data protection in the EU Legal order", *International and Comparative Law Quarterly,* (2014): 569-597.

[309] Directive 95/46, of the "European Parliament and of the Council of 24 October 1995 on the Protection of individuals with regard to the processing of personal data and on the free movement of such data", 1995 OJ (L 281/).

[310] Gregory Shaffer. "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of US Privacy Standards", 25 *Yale Journal of International Law*, (2000): 1.

for certain type of security relating to public and state affairs and criminal law.[311] It also explicitly deals with the data processed for business sectors. As compared to US and other countries the EU directive imposes some pre and post requisite to the data controllers for collection, processing and use of personal data in business spheres. The data controllers are directed to intimate the purpose of required information to the data providers and data receivers.[312] A data may be collected and transferred only for specified purposes.[313] Further, it also restricts the availability of certain type of data which may be considered sensitive. Such as information related to the religious beliefs, political opinions, racial and ethnic origins, health and sex life, gender, memberships and associations. Moreover, the Directive demands special permission from individuals before the disclosure of any sensitive information to the third party for business purposes. The Directive also provides the right of objection to such sharing and disclosure.[314]

The Directive further provides the right to individuals to question any decision regarding the transfer of any information and data acquired by automatic processed data systems.[315] This Directive also gives the right to make objection about the use of any data or information after processing it. It also provides the opportunity to observe and follow the data whether it is used for specified purposes or not. Similarly, it also gives the right to make corrections to the processed data and to update it. The individual may also collect the information and identities of third party which is demanding any data.[316] The Directive along with these rights gives the mechanism of

[311] Article 2-3 of EC Council Directive 94/46EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data (Privacy Directive), O.J.L. 281, (1995).
[312] Ibid; art. 10.
[313] Ibid; art. 6.
[314] Ibid; art. 14b.
[315] Ibid; art. 15.1.
[316] Ibid; art. 12.

enforcement to the member states. It provides that the member states shall have a local authority within its territorial boundaries to implement this directive and to collect and monitor such data[317]. The member states are further directed to provide legal remedies in case of any violation and damage to the provided information and data.[318]

This Directive of EU becomes the law of a member state only in the situation that the member state adopts it in its local legislation. The procedure of local legislation is different from state to state. The EU Directive requires the member states to transfer the data only to those third states which guarantees an adequate level of protection. This level of adequacy shall be maintained centrally by European Commission.[319] In this way the privacy Directive has control not even in Europe but also outside the Europe over the third states. However, the directive also gives some exceptions to the state which does not has any adequate level of protection but entered into a contract with data controllers regarding the protection of data, fundamental rights and freedom of individuals.[320]

3.5.2: The UN Guidelines on Data Privacy, 1990

The UN introduced the right to privacy first time in 1948 in an international document namely, the UDHR. Similarly, the right to privacy was also addressed in ICCPR in 1966. In both instruments the individual's right to privacy is made inviolable against any interference. It is also stated that the home, family and correspondence of a person shall also be protected from all forms of unlawful intervention. Moreover, the repute and honour of a person is also liable for the legal protection.

---

[317] Ibid; art. 22.
[318] Ibid. at art. 28.
[319] Ibid. at art. 25.
[320] Ibid. at art. 26.2.

The UN started its efforts to protect the computerized data and information in 1980. However, it took a long time to come on the page of "Guidelines for Computerized Personal Data Files, 1990".[321] These guidelines deal with various aspects of data protection of individuals. These guidelines also demand for the establishment of a national and local authority at state level to control the transborder flow of data.[322] It is also mentioned in the guideline that the member states which don't having the bilateral legislation on data transfer are not allowed to exchange the personal information of their individuals.[323] Directions are also narrated for the protection of such data which is deposited to international organizations systems.[324] The UN guidelines are the pioneer principles which deals with the protection of information gathered by the use of computers in spite of the fact that it took a decade to frame these rules.[325]

3.5.3 UN Special Rapporteur on the Right to Privacy in Cyberspace:

In today's time when the world is going to enter in the era where it is mandatory and indeed responsibility of the United Nations (U.N) and other regional organizations to work together on one agenda through which the terms would be defined unambiguously, the problems of investigation and prosecution are to be addressed along with the problem of jurisdiction. As the recent noticeable activity from the UN special rapporteur on the right of privacy urged that the world now needs to protect the privacy in cyberspace, as the cyberspace is no more secure from the cyberattack. He suggested that the state needs to cooperate with each other to gain high-rise in

---

[321] The "UN Guidelines Concerning Computerized Personal Data Files", G.A. Res. 45/90, U.N. Doc. A/RES/45/90 (1990).
[322] Ibid; Article 08.
[323] Ibid; Article 09.
[324] For instance, the EU only introduced a European Data Protection Supervisor in 2001.
[325] Christopher Kuner, "An International Legal Framework for Data Protection: Issues and Prospects", 25 *Computer L. & Security Review*. 314 (2009).

this field and it can only be possible when the regional cooperation and UN will work hard in a single direction in which each state would be given equal opportunity of research and expression. He said that the domestic governments must take initiative to deal with this serious issue. He also requested that the member states of UN have to ratify the data protection convention from there domestic legislative houses without unexplained delay. The purpose behind this ratification must be data protection and the protection of security of the state.

The definition and endorsement of the term "privacy" can easily be seen in the international documents, though the term does not have a pact definition but is legitimized through several international instruments. ICCPR endorses it through Article 17, while the UDHR through its Article 12 also reaffirmed in resolution 28/6 adopted by Human Rights Council, it is protected by several international instrument without a proper definition.

The special rapporteur also discussed that until the definition is not given, we cannot suggest the punishments for the offenders can't be defined and inflicted, he also ensured that he is in a dire will to draw the fundamentals of privacy, same is to be done without exaggeration. The privacy protection has long been a concern of international rapporteurs, same is enlightened there in the report that the states are now concerned about the privacy and are now interested to make some sort of change to legitimize it through legislation. The Special Rapporteur on the right to privacy focuses on the work done in the first three years of his mandate, with a particular focus on the work completed on surveillance and privacy, and reflects on the role and mandate of Special Procedures mandate holders. International organizations and the regional organizations are consulted by the special rapporteurs to ensure regional as well as international development in

privacy protection. The specialty of this task is that the rapporteur not only consult the governments but also consult the law enforcement agencies, the intelligence, forensic examiner etc.

Before going in deep, it is important to discusses the mandate and the procedure adopted by the special rapporteurs in formulating the aforementioned report, the special rapporteur conducted research on the several areas of his mandate, so matter is discoid under several heads. Firstly, the rapporteurs are to research diversely to gather diversified information and to recommend constructively for the promotion and protection of privacy and they also enlighten and enumerate the factors affecting it and the outcomes of the latest technology on it.

Emphasized on the given area, it is evident that the contribution of special rapporteurs is unprecedented as shown in the practical step adopted by U.N in 2013 when the General Assembly adopted the resolution 68/167, the credit goes to the special rapporteur's report presented after a deed extensive researches in which the negative impact of surveillance and interception of communication on human rights. The U.N enunciated that the people rights must be secured, the rights they have in offline status must be protected online beyond any sort of circumstances. It is important to mention here that after a great sufferings and heavy losses due to the terrorist attack it is pitiable to see the domestic response from not only developing countries but the developed countries as well no country has its domestic legislation that comply the international standards set out there in international instruments. The special rapporteurs from time to time shared with the international forums about the gradual progress, they contributed to a bridge the gap arising between different institutes and respond to the concerns.

3.5.4 The Asia Pacific Economic Cooperation (APEC), 2004

The Asia-pacific economic cooperation (APEC) is the first legal framework which provides far

reaching legal structure to ensure worldwide data privacy.[326] The APEC, in 2004 introduced its principles related to privacy of data.[327] These principles commonly known as privacy framework. In this framework there are nine principles regarding privacy and protection of data. These principles are flexible in nature as they are not binding upon member states.[328] These principles provide a framework for measures to protect the information of persons in member states. However, much advancement is yet required to meet the desired standard of privacy. It gives a layout of principles to those states where the adequate standard of privacy is not existing to combat the infringement of protection of data.

3.5.5 Role of South Asian Association for Regional Cooperation (SAARC) on the Issue of Cybercrimes:

The South Asian Association for Regional Cooperation shortly called SAARC is established on 8th day of December, 1985, the document that gave birth to it is SAARC Charter. There are eight member states of this body Afghanistan, Bangladesh, Bhutan, India, Maldives, Nepal, Pakistan and Sri Lanka. As far as the secretariat (the principal seat) of SAARC is concerned, it is situated there at Katmandu, the Capital city of Nepal, it was set up on 17th day of January, 1987.[329]

The glimpses of SAARC Charter indicate that the essence behind its formulation is the protection of the people inhabited in the region of South Asia, the objectives of the SAARC as per the SAARC Charter are as follow: -

---

[326] Extracted from <http://works.bepress.com/tim_wafa/> (Last accessed: 20 November, 2018).

[327] "The Asia Pacific Economic Cooperation Framework Order of 29 October, (2004)". Online available and retrieved from: http://www.cyberlawcentre.org/ipp/apec_privacy_framework/APEC_ Principles_local.htm. (Last accessed: 16 November, 2018).

[328] Graham Greenleaf, "Five Years of the APEC Privacy Framework: Failure or Promise?", 25 *Comp Law L. & Security Review*. 28, 37 (2009).

[329] The South Asian Association of Regional Cooperation (SAARC) https://www.saarc-sec.org/index.php/about-saarc/about-saarc (assessed September 27, 2020)

- It primarily protects the people of South Asia by promoting the quality of life of the people.
- To catalyze the economy of member-states, boost social progress of the people, contribute in developing the culture of the people of South Asia and to provide the people the rational to live a prosperous live by giving them proper equal opportunities so that they could judge their actual potential.
- The most important among all is strengthen the relation between the member countries by adopting the means of mutual trust, understanding and resolving one another's problem and to strengthen them on International forums and adopt the means to cooperate the international and regional institutes and organizations.
- Another attribute that attracts the researchers and International bodies that the decisions in SAARC are merely on the basis of consensus and unity, all member states are equal having equal protection of law and equal opportunities, neither any state claim as herself superior nor anyone has the Veto-power like the permanent members having the same in United Nations.[330]

As one of the prime functions of this regional body is to maintain the regional countries in cordial relationship and to maintain their relation with the international world. As far as the contribution of SAARC in this particular field is concerned, SAARC primarily functioned to improve the standard of life of the people of member states, after that it contributed in diminishing terrorism in certain regional zones, it also renter its services to smooth the trade among the member states and international world. It also played a vital and unprecedented role in improving the health and medication in the member states. More specifically the 11th summit of

[330] SAARC Charter, 8 December, 1985

SAARC held on 4-6th day of January through which it is declared that the peace, stability and security of South Asia is to be promoted together with the improvement of global security, the idea of disarmament is given and appreciated. SAARC prominent role is to regulate peace and prosperity among the member states, generally speaking if SAARC is claiming that the body is regulating peace in the region to ensure peace and security in the world, it means that the cyber issue is somewhere discussed, but as it is not directly discussed in any of the summit, as the South Asia has pre-basic unsolved solvable problems, food, health and medication, standard of living, peace and security, trade relations, which are considered as the necessities, it definitely planed something to address the respective aforementioned issue, but is remained unaddressed.

Conclusion

Cyberspace laws of different nations are examined in this chapter. These laws are examined in order to evaluate the legislation of developed countries. The US legislation is also advanced to safeguard the privacy of its citizens in virtual world. Such as ECPA, FERPA, Financial Privacy Act, FCRA, HIPPA, Videotape Privacy protection Act and COPPA are there to shelter the information and data of US citizens in various sectors of country. Further, the legal framework of Argentina, Canada, Germany, Australia, China, France and India are also discussed.

As in this chapter the concept and development of data protection in cyberspace technology is also discussed. Therefore, in this regard the different international agreements are examined to evaluate the need of privacy and data protection in cyberspace. This chapter examined those documents which provide privacy protection in the form of guidelines, such as the OECD and the APEC guidelines. It has been argued that these guidelines for privacy protection are based on

economic interests with regard to privacy protection as well as viewing it as one of a number of fundamental human rights. The European Union Regulations, the UN Guidelines and the APEC provide rules for member states to protect the information and data on digital devices and cyberspace. It is worth mentioning that the OECD guidelines and council of Europe' convention made initiative for data protection in cyberspace. Similarly, the role of UN Special Rapporteur on the right to privacy in cyberspace and the reports by the UN Rapporteur on the issue of cyberspace crimes are also debated. While referring to regional mechanisms, the role of South Asian Association for Regional Cooperation (SAARC) to prevent cybercrimes is also examined. It is concluded that Proper legislation is required to deal with the security and protection of individuals' privacy in virtual world. The developed nations are trying to secure the information on cyberspace. It is also significant to examine the existing cyber legislation of Pakistan. Therefore, the next chapter is devoted to evaluate the cyber laws in Pakistan. This chapter has debated on the international perspective of a legal framework on right to privacy. However, as the core of the thesis is specific to the case of Pakistan. The next chapter discusses right to privacy and cyber laws in Pakistan.

Chapter Four

Right to Privacy and Cyberspace Laws in Pakistan

Introduction

This Chapter focuses on right to privacy and cyberspace laws in Pakistan. It analyses the relevant legislation on the subject. It is a dilemma for all states to protect privacy and security of individuals in digital era. Though Pakistan has laws but implementation of such laws in true sense is a big challenge.[331] These laws, meanwhile, have both positive and negative implications on privacy rights in Pakistan and are, as such, considered the main instrument in this study for understanding the dynamics of privacy in the country. This chapter discusses these laws which deal with the cybercrimes particularly to the intrusion into information, data and right to privacy of a person in cyberspace. In this context, this Chapter is divided into four Sections. Section one analyses the development of Cyberspace Technology in Pakistan. Section two deals with the laws relating to the right to privacy in Pakistan by analyzing the provisions of various enactments in order to create context for further discussion. It also evaluates the cyberspace laws of specific sectors in Pakistan. Section three examines various legislations concerning cyberspace technology in Pakistan, such as, National IT Policy and Action Plan (2000), Electronic Transactions Ordinance (ETO), 2004, Prevention of Electronic Crimes Ordinances (PECO), 2007 & 2009, Prevention of Electronic Crimes Act (PECA), 2016 and so on. The limitations on right to privacy are discussed in Section four.

---

[331] Arshee Ahmed and Dr. Sadiq Ali Khan, "Cyber Security Issues and Ethical hacking in Pakistan". Online available at: https://docplayer.net/3634399-Cyber-security-issues-and-ethical-hacking-in-pakistan.html (Last accessed: 20 November, 2018).

4.1 Development of Cyberspace Technology in Pakistan

With the advancement of ICTs, Pakistan has also adopted the ways of digital world. A considerable population of Pakistan use the network of communication technologies to interact with other people within and outside the country. A report revealed that 70% of population is using mobile phones to transfer and receive the communication traffic while 11% population is the user of internet and its subscriptions.[332] To meet the demands of this huge volume of people fifty internet operational services are there in Pakistan[333] and about five telecom operators are working in the country.[334] Internet reliance has made the communications information and data to be available in cyberspace. Following ICTs are playing major role to develop the cyberspace in Pakistan;

4.1.1 Computers

The advent of computers and big data have become the part of our lives. The arrival of computer systems also served as a motivation for making individuals' data and information, a valuable commodity.[335] The more suitable capability of computer systems to collect large quantity of information has led them to cyber-crimes. They have also ability to process and disseminate a bulk of records which has hoarded in them with the help of modern technologies.[336] Computers have the ability to store information for a long-time frame and such statistics can be easily recalled and analysed with little or no effort. Organizations, therefore use computers to preserve data for various

---

[332] Report of World Bank, "Pakistan: Internet users (per 100 people)", The World Bank, (2013) http://databank.worldbank.org/data/reports.aspx?source=2&country=PAK&series=&period (Last accessed: 16 November, 2018).

[333] Report of Bytes for All Pakistan, "Pakistan's Internet Landscape", November (2013), http://content.bytesforall.pk/sites/default/files/MappingReportFinal%20-%20Published.pdf

[334] Pakistan Telecommunications Authority (PTA), "Cellular Mobile", 28 March, (2014), http://www.pta.gov.pk/index.php?Itemid=135 (Last accessed: 16 November, 2018).

[335] Peter Grabosky, "The Global Dimension of Cybercrime", *Global Crime* 6.1 (2004): 146-157.

[336] B Koops, "The trouble with European data protection law", 4(4) *International Data Privacy Law*, (2014): 250-261.

functions.[337] The speedy improvement in ICTs and computer networks, permit the transmission of information and data through networks.[338] This is a threat to the privacy of a person. The computers also serve as a weapon to get entry to the different records and in this way intervene into the privacy. For instance, it is the primary tool through which private information and data is collected which can be spread on the internet.[339] big data is mostly acquired from computers. It is defined as a large body of records saved in a laptop or computer system that may be retrieved as required.'[340] It operates like a digital filing machine. Governments and private entities hold information warehouses and big data that host big amount of personal information. These data warehouses aren't bodily warehouse that can be seen or perceived. They are commonly imaginary and often on internet which hosts volumes of records.[341]In Pakistan computer framework is frequently used by individuals, institutions and government.[342] The difficulty with regard to computers is that during most cases, individuals do not know that their personal information is being hosted on a database. They, therefore, may not recognize the way to maintain their data in case of harm and breach of privacy relating to information.

4.1.2 Internet and Social Media

The internet is a very useful tool within the society. It is a platform to perform numerous responsibilities which make life easier for a user. Yet, via its nature, it is a powerful tool utilized

---

[337] L.A. Bygrave, "The place of privacy in data protection law", 24 *UNSW Law Journal*, (2001): 277-283.
[338] J Kokott and C Sobotta, "The distinction between privacy and data privacy in the jurisprudence of the CJEU and EctHR", 3(4) *International Data Privacy Law*, (2013): 222-228;
[339] P.A. Bernal, *Internet privacy rights: Right to protect autonomy*, (2014): 200.
[340] S.C. Bennett. "The "right to be forgotten": Reconciling EU and US perspectives", 30(1) *Berkeley Journal of International Law*, (2012): 162.
[341] J Fishleigh, "Is someone watching you? Data privacy and protection: Current issues", 15(1) *Legal Information Management*, (2015): 61.
[342] Majid Yar, *Cybercrime and Society*, London: Sage Publications, (2006).

in exploiting people' private information. The internet, in spite of its numerous benefits,[343] causes one of the most serious threats to peoples' privacy. It has significant capacity to build up and keep large amount of personal data. Its capability to retrieve massive number of personal facts from the bulk of information in cyberspace makes it amazing. Search engines in the internet have very powerful sorting capabilities which offer the maximum accurate data about an individual without any laborious efforts to go through big efforts or manual filing structures. It creates the threats to individuals as a result of records processing on internet. therefore, many countries have enacted data privacy legal guidelines regarding the collections data from internet.[344]

Pakistan is ranked as sixth highly populated country of the world with around two hundred and twenty million humans. New media is rapidly flattering the part of the lives of Pakistani citizens, and specifically the entry into internet and the revolution in mobile industry has motivated their lives to an outstanding volume. In recent years, a remarkable rise has been seen in Pakistan in the use of Internet in general and in particular social media networking web sites. People of every age and gender are using the gadgets like cell phones, i-pads, and tablets with Internet facility.

They use new media for three purposes i.e. information, leisure and connectivity. Social media websites like Facebook, Twitter, Blogs, MySpace, YouTube, Viber and WhatsApp are in large part of the state are used for the purpose of Communication, interaction and connectivity. It is pertinent to mention that Pakistan has an extended IT industry, which is considered of giving a significance boost to the economic boom of the country in coming years. In Pakistan, there are

---

[343] Sally Richards, *Future Net the Past, Present, and Future of The Internet as Told By Its Creators and Visionaries*, New York: John Wiley & Sons, Inc., (2002).

[344] W. Servine and J. Tankard, *Communication Theories: Origins, Methods and Uses in the Mass Media*, New York: Longman, (2001).

around 100 million mobile users and 29 million internet users. According to an estimate, approximately 14 million consumers use mobile Internet. The persons, who have get admission to the Internet, are common users of social media. According to a survey carried out through Gallup Pakistan, a large majority (92%) of net users are normal consumers of social media. Since Pakistan is a male-ruled society, the male consumers are higher than to girls.[345]

It is pertinent to mention that Pakistan is one of the nations in the international community wherein adolescents are in majority. Around 62% population of the country is consisted of youngsters of age between 18-24 years.[346] A large majority of teenagers, especially urban inhabitants, is regular client of social media. Mostly, the social media equipment is used for the purpose of social interaction and political discourse. It is likewise used for e-commerce, socio-political deliberations and political activities. It is believed that the advent of recent media has enabled Pakistani young people to express their opinion publicly on various social and political dilemmas. Social media use has emerged as a trend in Pakistan and there are greater than 44 million social media accounts within the country. Facebook is the most famous amongst social web sites with 30 million customers throughout the world. The World Bank estimates that Internet penetration in Pakistan reached 10.9 % in 2013. The Internet Service Providers Association of Pakistan (ISPAK) estimated 25 million Pakistani users in October 2014. Among them 11.6 million Pakistanis are on Facebook.[347]

[345] Gallup (2016). Opinion Poll Information Technology Computer/Internet, Gilani Research Foundation, http://gallup.com.pk/wp-content/uploads/2016/06/30-June-2016-English1.pdf,

[346] S. Awan, "Some unfortunate aspects of social media in Pakistan", *Gender IT,* (2013).

[347] "Annual Social Media Marketing Infographics 2014", Pakistan Advertisers Society, 13th Jan. (2015).

4.2 Laws Relating to the Right to Privacy in Pakistan

Pakistan is a signatory to nearly all international treaties that consider privacy as a fundamental human right, including the UDHR, ICCPR and CRC but excluding the ICRMW. The 1973 Constitution of Pakistan recognizes "the individual's privacy as an inviolable right by specifically guaranteeing the dignity of citizens, privacy of home, the protection of life, liberty and body as fundamental rights. Provisions for privacy are further enunciated in the various laws of the country, subdivided into individual, informational and organizational domains.

Further, this section analyses the laws relating to the right to privacy in Pakistan by analyzing the provisions of Defamation Ordinance, 2002 and Defamation Bill, 2004, Freedom of Information Ordinance, 2002, relevant provisions of Constitution, 1973 and Pakistan Penal Code, 1860, Control of Narcotic substances Act. It also discusses terrorism and right to privacy and relevant provisions of the Arms Act, 1877, Prevention of Gambling Act, 1977 and West Pakistan regulation and control of loudspeakers and sound amplifiers ordinance in order to create context for further discussion.

4.2.1 Constitution of Pakistan, 1973

Constitution of Pakistan, 1973 guarantees the rights of the people of Pakistan. Article four[348] of the constitution secures the rights of every individual of the country. Article 4 (2) of the constitution prohibits all activities that are against to the life, freedom, body repute and property of any individual. Such activities may be taken as provided by law. Life of a person means the quality life not only quantitative life components. Life includes all necessary elements of life as

[348] It provides that: "(1) To enjoy the protection of law and to be treated in accordance with law is the inalienable right of every citizen, wherever he may be, and of every other person for the time being within Pakistan".

human being. Privacy is an essential component of freedom. It must be guaranteed to every human being. Life, freedom, repute and property are strongly connected to the privacy.[349] Therefore, it must be provided so that a person may live with security of his personal belongings.

The constitution of 1973 further ensures the right to life in the section of fundamental rights. It is stated in Article 09 that a person shall not be denied of his life and freedom except as it is permitted by law.[350] The constitution of 1973 provides the right to privacy to an individual. In Article 14 (1) it also ensures the dignity of every person and make it a fundamental right to secure his home from encroachment.[351] It states that "the dignity of man, subject to law, the privacy of home, shall be inviolable". Thus, the idea of privacy is enshrined in the fundamental rights of the people of Pakistan. As privacy is a key element of a person's life as he does not feel comfort to make his personal belongings or information to be public. Similarly, the notion of dignity is also made the basic right of an individual's life and it is connected with his privacy.

It is also worth mentioning that the constitution is the backbone of the legal framework of the country. It is the basic and supreme document of a nation. All rule and legislation are made in the light of this document. No law can be enforced in a country which is inconsistent to the provisions of constitution. All laws of a country must be directly or indirectly in accordance to the parent document that is the constitution of the state. In Pakistan, all laws are enacted in the light of the provisions of constitution of Pakistan, 1973.

---

[349] Volkman, Richard. "Privacy as life, liberty, property." *Ethics and Information Technology* 5, no. 4 (2003): 199-210.

[350] Article 09 of constitution, (1973) states that. Security of person: "No Person shall be deprived of life or liberty save in accordance with law"

[351] Article 14 (1) of constitution, (1973); Inviolability of dignity of man.

The constitution also asserts that the laws which will be against or conflicting to the fundamental rights of people shall be void[352]. In this way, it guarantees the rights of people in broader spectrum. However, some limitations are imposed in order to maintain law and order situation in the country and to provide justice. The constitution of Pakistan states that the Islamic provisions shall followed to make the legislation. Article 227, provides that all present laws shall be made in accordance to the injunctions of Islam as available in Holy Quran and Sunnah. Its further states that the laws which will be against to the injunctions of Islam shall be void[353]. The right to privacy is also enshrined into the teachings of Islam as mentioned earlier in chapter two. Therefore, the right to privacy must be secured in legal framework of cyberspace.

4.2.2 Inventory of Pakistani Laws with Reference to Privacy

The following section is comprised of the inventory of laws and regulations of the overall scenario governing privacy rights in Pakistan. A brief description of these laws is presented along with the relevant judicial cases, wherever applicable.

Pakistan Penal Code, 1860

Pakistan Penal Code is the substantive law of the Pakistan which provides the definitions and punishments for the offences. It is in vogue with the birth of Pakistan. It provides the comprehensive provisions related to the infringement of privacy. The offence of criminal trespass

---

[352] Article 8 deals with "Laws inconsistent with or in derogation of fundamental rights to be void. (1) Any law, or any custom or usage having the force of law, in so far as it is inconsistent with the rights conferred by this Chapter, shall, to the extent of such inconsistency, be void. (2) The State shall not make any law which takes away or abridges the rights so conferred and any law made in contravention of this clause shall, to the extent of such contravention, be void. (3) The provisions of this Article shall not apply to: - (a) any law relating to members of the Armed Forces, or of the police or of such other forces as are charged with the maintenance of public order, for the purpose of ensuring the proper discharge of their duties or the maintenance of discipline among them".

[353] Article 227 states that: "Provisions relating to the Holy Quran and Sunnah. -(1) All existing laws shall be brought in conformity with the Injunctions of Islam as laid down in the Holy Quran and Sunnah, in this Part referred to as the Injunctions of Islam, and no law shall be enacted which is repugnant to such injunctions".

is defined briefly in PPC and in this way safeguards the privacy of one's home. Criminal trespass is defined by unlawful entry or lawful entry made unlawful by illegal stay on a person's property with the intention to commit an offence or to insult, intimidate or annoy.[354] Similarly, the criminal trespass of a house, human dwelling, building and place of worship is referred as house-trespass.[355] Thus, the privacy of a home is secured. Further, the offence of house trespass after making the precautionary measures of concealing himself from owner or such person who having right to expel him from house is also made punishable in PPC under the head of lurking house trespass.[356]

The privacy of home is made more secured by incorporating advanced provisions of lurking house trespass by night i.e. before sunrise and after sunset. Furthermore, house breaking at night is also defined and made in PPC.[357] Sections 447-462 deal with the punishments of trespassing into one's property. Thus, these provisions of PPC directly deals with the trespass and have indirect connection with the right to privacy in cyberspace.

The Arms Act, 1878[358]

This Act was promulgated in 1878. Article 25 of this Act authorizes the magistrate, or any officer empowered in his behalf to make search and seizer of arms from any premises. The magistrate is

---

[354] Section 441 of PPC provides for Criminal trespass and provides that: "Whoever enters into or upon property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property, or, having lawfully entered into or upon such property, unlawfully remains there with intent thereby to intimidate, insult or annoy any such person, or with intent to commit an offence, is said to commit criminal trespass".

[355] Section 442 of PPC provides for House-trespass and states that: "Whoever commits criminal trespass by entering into or remaining in any building, tent or vessel used as a human dwelling or any building used as a place for worship, or as a place for the custody of property, is said to commit house-trespass".

[356] Section 443 relates to Lurking house-trespass and provides that: "Whoever commits house-trespass having taken precautions to conceal such house-trespass from some person who has a right to exclude or eject the trespasser from the building, tent or vessel which is the subject of the trespass, is said to commit lurking house-trespass".

[357] Section 446 provides for House-breaking by night and states that: "Whoever commits house-breaking after sunset and before sunrise, is said to commit housebreaking by night".

[358] Online available at: http://www.ma-law.org.pk/pdflaw/THE%20ARMS%20ACT.pdf. (Last accessed 20 November, 2018).

required to record reasons to believe of presence of such arms.[359] These provisions allow the magistrate and other officers to interfere into others' privacy but at the same time it demands reasonable believe for doing so.

West Pakistan Regulation and Control of Loudspeakers and Sound Amplifiers Ordinance, 1965[360]

This ordinance provides the safety of persons and their privacy while imposing restriction on the use of loud speakers or sound amplifiers in public place or residential areas.[361] Privacy, as it has been already defined, is a state of not being interfered by others. It is also a desire to be let alone or solitude. In this way, this ordinance ensures individuals' right to privacy by preventing noise and audio distraction in one's life.

Anti-Terrorism Act, 1997

Pakistan is in the front line of war against terrorism. After the incident of the US 9/11attacks, Pakistan is facing terrorist occurrence which has divided Pakistan into ethnic, socio-cultural, provincial, linguistic and ideological frontages. It resulted into state of insecurity for country as well as for citizens. South Asia Terrorism Portal database reported that since 2002 to 2011 there had been 9,620 civilian and 3,443 security forces mortalities because of terrorism.[362] Pew Global

---

[359] Section 25 of the Arms Act, (1878).

[360] http://www.pakistansocietyofcriminology.com/Admin/laws/TheWestPakistanRegulationandControl.pdf. (Last accessed: 20 November, 2018).

[361] Article 2 (1)(a) of West Pakistan Regulation and Control of Loudspeakers and Sound Amplifiers Ordinance, (1965).

[362] *"Pakistan Assessment Report (2011)"*, Online available and retrieved from: http://www.satp.org/satporgtp/countries/pakistan/. (Last accessed: 20 November, 2018).

Attitudes survey reported on July 29, 2010, that 98% of Pakistani believe terrorism as a great danger to the life of a person in country.[363]

This war has made people to be confined to the houses and made their privacy and liberty more vulnerable. People have the fear of physical losses of property, life and liberty. Pakistan's ranking in the world was at second number according to the 2010 report of Maplecroft's Terrorism Risk Index.[364] However, according to the report of Institute for Economics & Peace "Global Terrorism Index 2020: Measuring the Impact of Terrorism, Sydney"; Pakistan is at 7th number.[365] In addition to it, there are a number of provisions provided in national and international agreements, as well as domestic laws in which the right to privacy is compromised. There is a dire need to maintain the balance between security and privacy.

Anti-terrorism law was present at the time of independence of Pakistan. However, it was substituted by Anti-Terrorism Activities Act in 1975. In 1997 anti-terrorism Act was made that was amended and updated from time to time. The right to privacy however is protected in this Act. Law officers may enter and search the houses of the people.[366] They may also take the possession of any weapon or written material[367] which is doubted to be used in terrorism activities. It allows police officers to search on the ground of suspicion and reasonable believe to be searched.

---

[363] *"Concern About Extremist Threat Slips in Pakistan. Pew Global Attitudes Project"*. Online available at: http://pewglobal.org/2010/07/29/concern-about-extremist-threat-slips-in-pakistan/. (Last accessed: 20 November, 2018).

[364] *"Review of Maplecroft's "Terrorism Risk Index 2011" Terrorism"*, *Online* available and retrieved from: http://terrorism.foreignpolicyblogs.com/2010/12/04/review-of-maplecrofts-%E2%80%9Cterrorism-risk-index-2011%E2%80%9D/. (Last accessed: 20 November, 2018).

[365] Institute for Economics & Peace. Global Terrorism Index 2020: Measuring the Impact of Terrorism, Sydney, November 2020. Available from: http://visionofhumanity.org/reports (Last accessed: 30 March, 2021).

[366] Article 05 of Terrorism Act, (1997).

[367] Ibid; Article 10.

The security of Pakistan Act, 1952 enables the federal government to arrest any person who has acted in such way as inconsistent to the integrity, defense or security of Pakistan. His movements may also be restricted or ordered to be reported to any officer or authority.[368] The federal government may control subversive association and order to suspend its activities not exceeding for three months. It may also take the possession of any written material which it thinks to be used against the security of Pakistan. But all these restrictions are imposed in the safeguard of national security and integrity of state as no such restriction shall be imposed without justifiable reasons.[369]

The Prevention of Anti-National Activities Act, 1974 provides the definition of anti-national activities including the questions, disclaims or disruption of sovereignty of Pakistan. Such activities are in contradiction to the measures as taken by federal government to curb the terrorism.[370] Individual's right to privacy is in danger according to the provisions of this Act. It is the discretion of federal government to declare any activity as anti- national without the judicial involvement.[371]

Further, the federal government may order any officer to enter into the premises of any person and to make investigations relating to money, securities or credit. In such case the order of investigation shall be the warrant.[372] These unfettered powers of federal government shall be used appropriately and without any compromise upon privacy of individuals.

---

[368] Article 03 of Security of Pakistan Act, (1952).
[369] Ibid; Article 10.
[370] Article 02 of The Prevention of Anti-National Activities Act, (1974).
[371] Ibid; Article 03.
[372] Ibid; Article 07 (2).

All these searches shall be carried out only with the prior permission of federal government and in this way the right to privacy of a person is secured. Moreover, these searches are carried out under the provisions of law. Arbitrary and unlawful interference is completely banned.

Prevention of Gambling Act, 1977

It was enacted in 1997 and in pursuance of this Act the provinces have also the same legislation in the name of ordinances. Certain provisions of this Act are directly related to the right to privacy. As it is mentioned that search may be made to the premises used as gambling den but such power is conferred to district magistrate or magistrate of first class. This search requires the prior information that the premises is used for gambling. Further, it gives opportunity to allow females to leave the place.[373]

Quetta High Court, Baluchistan held in *Ghulam Hussain vs. Additional session Judge, Dera Allah Yar*[374], the magistrate was not present at the time of raid. The police had not authority to search the house under Baluchistan Prevention of Gambling Ordinance, 1978.[375] Police has to assist the magistrate only. The provisions of section 08 are violated and the privacy is infringed. Constitution also ensures privacy of home[376] and teachings of Islam also endorse the right to privacy. In the said raid the formalities are not observed that's why the material seized in raid not relied on. Accused is innocent and acquitted.

---

[373] Section 08 of Prevention of Gambling Act, (1977).
[374] *Ghulam Hussain vs. Additional session Judge*, Dera Allah Yar, *(2010 PLD 21)*
[375] Ibid; para 95.
[376] Article 14 of Constitution, (1973).

Control of Narcotic Substances Act, 1997[377]

This Act came into operation in 1997. It was drafted to make provisions about narcotic and psychotropic substances. Individual's right to privacy is infringed by its various provisions. The powers and procedures provided for making arrest and investigations are direct implication on the privacy of persons. They may be searched at any time of day or night by an officer having warrant of arrest issued by special court.[378] The officer may also use force if it is desired while searching the person. A sub inspector or other high-grade officers may arrest a person without warrant of special court if such officer has reason to believe that the narcotics substance is present and the suspect may be escaped or evidence may be damaged if the time is spent on obtaining the warrant. To eliminate the corruption or misuse of power the Act also required to write the reasons of suspicion and grounds of information. The copy of this record should be forwarded immediately to his senior officer.

In *Arshad Hussain vs. State,* it was held by the High Court that the magistrate was never empowered to enter into home without due process of law and prior permission of residents. Association of magistrate with raiding persons is of no importance unless it is followed by legal provisions. As privacy of the house may be proceeded as criminal trespass and damage to privacy. Section 23 of the Act empowers an officer, who is mentioned in section 19, to stop and search any conveyance or vehicle on road or in the air and to examine it for narcotics substance.[379] However, the rank of such officer is not mentioned anywhere even in section 19.

---

[377] http://www.fmu.gov.pk/docs/laws/Control%20of%20Narcotic%20Substances%20Act.pdf (Last accessed: 20 November, 2018).
[378] Section 20 of Control of Narcotics Substance Act, (1997).
[379] Ibid; Section 23.

The Right to Access to Information Act, 2017[380]

Right to information is a key right provided by the UDHR. This right is also incorporated in Pakistan's legislation "The Right to Access to Information Act, 2017". This right is installed to make government institutions more transparent and efficient. Accountability is done to make departments more elevated. This right is used to increase the standards of governance of a nation. On the other hand, this right is in contradiction of right to privacy. Individuals' data is more sensitive and critical. However, to combat the issue of interference with the privacy of an individual certain provision is imbedded in this Act. Three types of records are exempted to be made public.[381] First, the records of banks and financial institutions with regard to their customers are exempted to be made public;[382] second, the individual's record with reference to his privacy is excluded[383]; and third, the private documents provided to public body are also exempted.[384] Baluchistan and Sindh[385] provincial legislations have also imposed the same limitation over the information rights to secure the individual's right to privacy.

The National response center was also established to control the misuse of internet and to secure the cyberspace from criminals. In 2002 government ordered the PTA to keep and monitor the record of cyber cafe users. The report says that, "Gen Musharraf says his government has invested more than 100 million euros in communications and sharply reduced the cost of connections and services since 1999". Another endeavor taken by this center was the blocking of

[380] Pakistan - The Right to Access to Information Act, (2017).
[381] Section 8 of The Right to Access to Information Act, (2017).
[382] Ibid; Section 8 (d).
[383] Ibid; Section 8 (g).
[384] Ibid; Section 8 (h).
[385] Balochistan FOI Law, "Campaign for Freedom of Information", Pakistan. Online available at: http. www.ourrighttoknow.org.balochistan-foi-law html. (Last accessed: 20 November, 2018).

websites containing anti-Islamic, blasphemous, unethical and pornographic data as it does not come under the preview of right to privacy.

Defamation Ordinance, 2002 and Defamation Act, 2004

The defamation ordinance 2002[386] and the defamation Act 2004 provide security to an individual's interest. The clauses of section 499 of PPC are hereby replaced by these enactments. According to this legislation, defamation is the injury to the reputation of a person by wrong statements or publication. It may be in the form of written or verbal statements. Any written material used to defame a person's integrity is known as libel while oral stamen is referred as slander.[387] In this way the privacy of a person is also disturbed when the repute is infringed.

Karachi High Court, Sindh held in *Shariq Saeed vs. Mansoob Ali khan*[388], one should keep in his mind that the freedom of speech and right of expression are not the unfettered and unbridled rights. One must be kept in his mind the provisions of Article 14 of constitution while exercising his right of speech and right of expression. Moreover, it should also be remembered that freedom of speech and expression impose a correspondence duty to maintain the boundaries of Article 14 of constitution of Pakistan.

4.2.3 Sector Specific Laws Dealing with Right to Privacy

Pakistan Medical & Dental Council Code of Ethics [389]

This code of ethics protects the right to privacy of a person. The physician is bound to not disclose the information provided by patient with regard to his ailment or treatment. The relation between

---

[386] http://www.intermedia.org.pk/mrc/medialawdocs/defamation-law.pdf. (Last accessed: 20 November, 2018).
[387] Article 3 of the Defamation Ordinance, (2002).
[388] *Shariq Saeed vs. Mansoob Ali khan*, 2010 YLR 1647.
[389] http://www.pmdc.org.pk/Ethics/tabid/101/Default.aspx. (Last accessed: 20 November, 2018).

doctor and patient is trust based. The doctor should protect the information of his patient as it may injure the repute of his patient if it is disclosed. Section 5 of the code[390] deals with oath of doctors and dental practitioners. This code bounds the doctors to not share their patient's information with others.[391] Doctors are not under any legal obligation to share this information and it is the privileged communication between him and his patient[392], therefore, no government body can demand this information.[393] However, the court may require this information as relevant fact or fact in issue in any proceedings before it.[394]

Banking Companies Rules,1963[395]

These rules ensure the individual's right to privacy in financial transactions. The state bank of Pakistan is required to publish information only in the public interest or at time of elections of persons when the payments of any loan or credit has been due more than one year.[396]

State bank issued a circular for banks to provide information of customer's account to central board of revenue with their names, account details and tax payments. The Lahore high court held in *M.D. Tahir, Advocate vs. The Director, State Bank of Pakistan* that such circular is not legal on account of subordinate legislation. It stated that it will be the infringement of privacy without any wrong doing. It also asserted that it is against the provisions of constitution.[397] High court struck down the circular.

---

[390] Section 5 of Pakistan Medical & Dental Council Code of Ethics
[391] Ibid; Article 12.
[392] Ibid; Article 12.1
[393] Ibid; Article 12.2
[394] Ibid; Article 12.3
[395] http://www.sbp.org.pk/publications/prudential/ordinance_62.pdf. (Last accessed: 20 November, 2018).
[396] Article 33 of Banking Companies Rules, (1963).
[397] Article 4 and 25 of Constitution, (1973).

Press Council of Pakistan Ordinance, 2002[398]

This ordinance imposes the ethics on press under the administration of press council. Press council has the duty to enforce the code of ethics according to the rules related to the privacy.[399] The ethical code is provided in the schedule of ordinance. In the code five articles deal with privacy. Any defamatory publication against the repute of a person is banned.[400] Any interference into the privacy of person, home or family is not allowed.[401] Discrimination and hatred speech are prohibited.[402] The names and photos of women and children who are sexual victims should be concealed.[403] The background interviews and discussion shall be kept confidential.[404]

4.3 Legislations Regarding Cyberspace Technology in Pakistan

The major challenges to control cybercrimes 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 transborder nature of cybercrimes criminals are more privileged to commit these threats.[405]

---

[398] http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/Pakistan%20Press%20Council%20Ordinance%202002.pdf. (Last accessed: 20 November, 2018).
[399] Article 08 of Press Council Pakistan Ordinance, (2002).
[400] Ibid; Article 1.
[401] Article 4 of Press Council Pakistan Ordinance, (2002).
[402] Ibid; Article 7.
[403] Ibid; Article 14.
[404] Ibid; Article 15.
[405] Ghulam Muhammad Kundi, Bahadur Shah and ALLAH Nawaz, "Digital Pakistan: Opportunities and challenges", *Journal of Information Systems and Technology Management*, Sao Polo, Brazil, 5(2): 365-390, (2008).

According to a survey, almost 10 to 15 cases are reported[406] on daily basis related to cyber-crimes involving illegal funds transfer, password cracking, account hacking, salami attacks and internet spoofing. To combat these crimes Pakistan has made several laws. But there is no uniform pattern for data privacy legislation in cyberspace. Laws of Pakistan are not enough to deter the criminals from committing cybercrimes. In this regard no, considerable success has been attained to make cyber environment free from threats.[407] Despite of the fact that Pakistan is signatory of various international instruments, the Government of Pakistan has not designed cyberlaws in harmony to the international laws yet. Pakistan has made following cyber laws till now.

The Telegraph Act, 1885 [408]

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.[409] In the name of public interest unbridled powers are exercised by government without the intervention of courts. The government may take the possession of telegraph in case of public emergency and for public safety. Anyhow some penalty is also imposed if someone enters into telegraph offices[410] and interferes with telegraph message unlawfully.[411] The punishments for annoyance of telegraphs are same for general public and government officials.[412]

---

[406] Ullah, Sultan, Muhammad Amir, Mudasser Khan, Hamid Asmat, and Kamran Habib. "Pakistan and cyber crimes: Problems and preventions." In *2015 First International Conference on Anti-Cybercrime (ICACC)*, pp. 1-6. IEEE, 2015.

[407] S. Awan, "Some unfortunate aspects of social media in Pakistan", *Gender IT*. (2013).

[408] http://www.pakistansocietyofcriminology.com/Admin/laws/TelegraphAct1885.pdf. (Last accessed: 20 November, 2018).

[409] Article 05 of The Telegraph Act, (1885).

[410] Ibid; Article 23.

[411] Ibid; Article 24.

[412] Ibid; Article 25-d.

Pakistan Telecommunication (Re-organization) Act, 1996[413]

This Act provides that the Telecommunication Authority or the Frequency Allocation Board should inform the court about any illegal act regarding telecommunication. The court has the power to issue warrant for search of such premises where illegality is done, to seize such equipment used for crime or to make investigations.[414] Thus, the involvement of the court is a good step to ensure the privacy rights of people. However, it is in contradiction of security Act which empowers the federal government to tap calls of citizens for the security of national interest or to combat the crime in case of apprehension of offence.[415]

A person's privacy may be disturbed for an unlimited period of time in apprehension of offence. However, this Act did not give permission of any suit or proceedings against the authority or its employees for the acts done in good faith.[416] This is an impediment on the privacy and others rights of persons. As no accountability is imposed on members and employees of authority. They may misuse this unfettered power under the umbrella of good faith and thus damaging the both, privacy and reputation of an innocent person. A logical complaint system must be introduced with enough evidence as to satisfy the court for not infringing the privacy.

PTA Telecommunication Rules, 2000[417]

These rules are related to the right of peoples of Pakistan. As they address the terms of granting licenses and other related services. They also provide privacy and protection to customers while dealings with telecommunications networks. The PTA Telecommunication Rules of 2000 is a

[413] http://www.privatisation.gov.pk/PDF-Files/Telecom%20Act.PDF. (Last accessed: 20 November, 2018).
[414] Section 32 of Pakistan Telecommunication Act, (1996).
[415] Article 54 of National Security Act, (1947).
[416] Section 33 of Pakistan Telecommunication Act, (1996).
[417] http://www.pta.gov.pk/media/rules_280208.pdf. (Last accessed: 20 November, 2018).

document governing the relationship between the authority (PTA) and the licensee. The document is comprehensive and elaborates the codes and procedures that need to be followed while granting licenses and associated services. These rules are important for discussion as telecommunication governs the lives of almost a million people across Pakistan.

These rules provide certain conditions in the annexed schedule[418] which are linked with the confidentiality and protection of customers information.[419] Customers information shall not be compromised without his consent.[420] *Mohtarma Benazir Bhutto and Others vs. President of Pakistan and Others*[421], Supreme Court held that telephone tapping and spying on communication[422] is against the constitutional protection of life[423] and privacy[424]of a person. Telecommunication laws for tapping the calls of people are needed to be updated to protect the infringement of constitutional rights. Tapping shall be done with permission of Supreme Court or a commission established by Supreme Court. Such tapping and spying shall not be made more than six weeks and the order shall be reviewed forthwith on the expiry of this period.

National IT Policy and Action Plan, 2000[425]

Pakistan Government adopted its IT 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. Guidelines and models related to cyberspace and internet authenticity were approached to design this policy. After

---

[418] Schedule 02 of PTA Telecommunication Rules, (2000).
[419] Ibid; Section 04.
[420] Ibid; Article 4.2(a).
[421] *Mohtarma Benazir Bhutto and Others vs. President of Pakistan and Others*, (PLD 1998 SC 388).
[422] Article 54 of National Security Act, (1947).
[423] Article 09 of Constitution, (1973).
[424] Ibid; Article 14.
[425] Online available at: http://investinpakistan.pk/pdf/National_IT_Policy.pdf (Last accessed: 20 November, 2018).

reviewing the approaches adopted by other countries, the "International Consensus Principles on Electronic Authentication" designed by Internet Law and Policy Forum was deemed good to be followed to make this policy.[426]

Privacy right is secured in IT Strategies section of the policy. It provides the safeguard to the privacy of individuals and to keep their transaction secret. It even restricts the state to interfere into the privacy of citizens, except to be proceeded in the legal domain if it is required. I.T policy and action plan is made to make the privacy of individuals more secured and to protect the way of E-commerce.[427] This instrument is a milestone to make the cyberspace secure.

Electronic Transaction Ordinance, 2002

This ordinance was promulgated in September 2002. With the advent of information and communication technologies, the day to day transactions have been shifted to digital era. From entertainment to health, education to business, government to military, every sphere of life has become dependent on internet and technology. Business transactions have been shifted from hype of pages to digital era. 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.[428]

Before the enactment of PECA, 2016 the two sections 36 and 37 respectively of ETO, 2002 were in operation in order to safeguard the information of persons. All type of information privacy was guaranteed in these two provisions. Violation of privacy in information systems[429] or damage

---

[426] Khalil-ur-Rehman Khan. "Cyber Laws in Pakistan". Online available and retrieved from: https://www.scribd.com/document/203767010/Cyber-Laws-Pakistan (Last accessed: 20 November, 2018).
[427] Article 3.4.12.2, I.T Policy Strategies.
[428] Ibid;
[429] Section 36 of ETO, (2002).

to the information[430] were recognized as offence in ETO, 2002. However, with the promulgation of PECA, these provisions of ETO has been lapsed in the domain of privacy[431] and protection of data in information systems.[432] Further, this ordinance suggests the Federal Government to make rules for the protection of data and to secure the privacy of the users but no step in this regard has been taken yet.[433]

The PECO Ordinances, 2007[434] and 2009[435]

This ordinance has been lapsed. However, it was made to prevent the breach of privacy, to maintain confidentiality, to protect information and data, to safe information systems from intrusion and to provide punishments for the breach of its provisions. It also provided the procedure of investigation and prosecution of offences. This ordinance was directly related to the privacy of individuals and protection of their information on electronic systems. Unauthorized access to any information system was declared as criminal access.[436] It also prevented unauthorized access to any information and data contained in an electronic device or system.[437] Access to password and codes to gain data and information declared an offence.[438] Distribution and transmission of Malicious codes was also made a crime as it directly intervenes in privacy of other persons.[439]

Forwarding of bulk of messages known as spamming was also made an offence as it encroached in the privacy of others.[440] Unauthorized interception was also addressed as an offence

---

[430] Section 37 of ETO, (2002).
[431] Section 36 of ETO, (2002).
[432] Section 36 of ETO, (2002).
[433] Article 43 (2) (e) of ETO, (2002).
[434] Online available at: http://www.fia.gov.pk/electronic_prevention_orde.pdf. (Last accessed: 20 November, 2018).
[435] Online available at: http://www.fia.gov.pk/electronic_prevention_orde.pdf. (Last accessed: 20 November, 2018).
[436] Article 03 of PECO, (2007).
[437] Ibid; Article 04.
[438] Ibid; Article 10.
[439] Ibid; Article 12.
[440] Ibid; Article 14.

as it attack the personal information of and individual which may cause damage to his life, money, property, repute and family.[441] Under this Ordinance, the Federal government was empowered to investigate the online activity of a person related to specific correspondences and communications which is the direct concern with the right to privacy. Moreover, the service provider were made authorized to retain the information if it was required by Federal Government.[442] Such information was liable to be acquired without the consent of user and would be kept confidential from him. Judiciary is not involved for the collection of such real time data under this Ordinance.

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 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 country. Cyber stalking, cyber spoofing, fishing, cyber harassment, illegal access to information system[443] or device, illegal access to information or data[444], illegal interference with information or data[445], illegal interference with information system[446], cyber terrorism[447], blasphemy and cyber forgery[448] are introduced as cyber-crimes in the Act. However, the language of the Act is not plain and clear. It is the opinion of many human rights organizations[449] and legal experts that the language of the

[441] Ibid; Article 16.
[442] Ibid; Article 27.
[443] Article 03 of PECA, (2016).
[444] Ibid; Article 04.
[445] Ibid; Article 5.
[446] Ibid; Article 06.
[447] Ibid; Article 07.
[448] Ibid; Article 08.
[449] Online available at: https://www.privacyinternational.org/node/881 (Last accessed: 20 November, 2018).

act is required to be more specific and this burliness intervenes into the privacy as well as compromise the freedom of expression[450].

Under this Act, whoever uses the identity of another person to commit any fraud is liable of intrusion into privacy of a person[451]. The transmission of one's identity information for the purpose to be used in any offence of fraud, deceit or falsehood is also infringement of the right to a person's privacy.[452] 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 the breach of privacy.[453] Law enforcing agencies may intercept any information in order to make national security. However, the privacy is compromised in this situation.

Further, the Court may issue 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.[454] The court may also issue warrant to a person who is in the possession of such data resulted from specified communication to share data within seven days which it believes to be required for the investigation purpose[455]. This section is also related to the right to privacy but in the whole Act specified communication is not discussed.

Moreover, the service providers have the authority to retain data for a minimum period of one year[456] that is a clear impediment to the right to privacy and protection of information. Pakistan

---

[450]Online available at: http: www.ohchr.org Documents Issues Opinion Legislation PAK_2016.pdf(Last accessed: 20 November, 2018).
[451] Section 11 (1) of PECA, (2016).
[452] Ibid; Section 11 (2).
[453] Section 12 of PECA, (2016).
[454] Ibid; Section 19.
[455] Ibid; Section 20.
[456] Ibid; Section 29.

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.[457] 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.[458] 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 investigation with foreign intelligence agencies without intervention of court. It is discretion of federal government to seize and share such data however; no internal human right document is highlighted to support these provisions.[459] 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 behaviour in cyberspace. Funds are to be allocated for the establishment of forensic laboratories and cybercrime police stations. This Act operates in both ways i.e. to protect the individuals and to protect the state. Individuals can seek justice against crimes like identity or data theft.[460]

To some extent, the 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.[461] However, the present Act is not sufficient to secure the privacy of individuals. Moreover, this Act is not supported with any

[457] Ibid; Section 34.
[458] Ibid; Section 30.
[459] Ben Emmerson, "the UN Special Rapporteur on counter-terrorism and human rights, Two years after Snowden: protecting human rights in an age of mass surveillance", Executive summary, Report of Amnesty International, (2015).
[460] Online available at: https://www.dawn.com/news/1288627 (Last accessed: 20 November, 2018)
[461] Section 13 of PECA, (2016).

updated data protection laws. Similarly, no commission is established to safeguard the privacy and protection of data and information of people.

4.4 Limitations on right to privacy in Pakistan

Followings are the limitations on the right to privacy.

Code of Criminal Procedure, 1890

In this code certain restrictions are imposed to make a document to be public or to be able for privacy. According to section 99-A, if a document is prejudicial to the national integrity or against the government then it shall be liable to forfeiture and the court is empowered to issue the search warrant for such document. lt is declared in this section that the privacy of a document is not ensured which is against the national interest. Further, the court has a power to consider any document liable to forfeiture if it is prejudicial to national interest.

Similarly, the ambit of this section is strictly narrowed around the certain documents. Which are restricted to become public on the ground of being injurious to national integrity.[462] To prevent the abuse of this section it is clearly stated that the information about the government acts is not liable to be dealt under these provisions. It is also declared that the acts of government and the functions of government officials are not detrimental to national interest within the preview of this section. In this regard the Sindh High Court stated that the order should specify the reasons for forfeiture of a certain document under section 99-A. it is clearly mentioned in the said decision

[462] *PLD 1961 KAR.129.*

that the document must be seized on a valid reason otherwise no interference into one's privacy is allowed.

The Lahore High Court, in its judgment explained that the documents cannot be taken into custody without valid reason. If a document is forfeited it must contain certain provisions which are rendered against national integrity. Further it stated that the federal government should explain a document as being against the law before declaring its forfeiture. Furthermore, it is also stated by the High Court that the document must contain some objectionable material that has been published intentionally to harm the repute of another person. The order under this section needs to be made with great caution. As it may happen that the publication is not made to harm any person.[463]

It is noticeable that the documents are seized only on the ground of being against national interest. Moreover, the reasons are needed to be mentioned clearly in the order so that a person may be satisfied. The aggrieved person should be told the sufficient reasons for such order. However, the provisions of the section 99-A are required to be more comprehensive and specific. So that the term "prejudicial to the national integrity" may be taken into real sense and the documents are not forfeited without justified reasons. Moreover, the right to privacy and freedom of information may also be balanced in this way.

Section 352 of the code of criminal procedure 1890, states that the trials shall be conducted openly and before the public. This section provides opportunity to those persons who want to attend the proceedings of the trial. The proviso of this section empowers the Presiding judge or Magistrate to forbid any person to attend the proceedings of trial. It is not mentioned in this proviso

[463] *PLD 1960 LAH.629.*

that on which ground a person may be prohibited to join the proceedings of court. It was held by the Supreme Court of Pakistan that the it is necessary for the administration of Justice that it should not only be done but appear to be done. So, the trial must be held in an open court. The public shall have open access to attend the proceedings. This practice is required to promote the justice, equality, uprightness and confidence in the law courts. This section is a limitation over the right to privacy of a person. A person who is not interested for a trial in open public, is aggrieved by the provisions of this section. It is needed to be amended so that it may be clear that on which grounds the court has a power to restrict any person to participate in a trial. However, open trial is beneficial for public welfare. In this way, people become more confident to rely on courts. Further, in open trials the people have access to information. But on the other hand, it is not in favour of privacy.

The Constitution of the Islamic Republic of Pakistan, 1973

Before 18th amendment, there was no explicit right to information in the constitution of Pakistan, 1973. Article 19 of the constitution deals with freedom of expression and speech. It was interpreted by the Supreme Court of Pakistan as a freedom of information.[464] In the constitutional petitions 77 to 85/89 usually referred as Memogate Scandal the Supreme Court stated that the petitioners, respondents and their lawyers are not vigilant about their constitutional rights.[465] They have overlooked the gross change about the right of information. It is a realty of our history that since after independence people are kept deprived and they are not granted the freedom of information. However, such information may be really important for them. This right is justified by the courts of Pakistan while interpreting the provisions of constitutions. In *Nawaz shareef vs. President of*

[464] *Mian Muhammad. Nawaz Sharif vs. President of Pakistan and others (PLD 1993 SC 473).*
[465] The Supreme Court of Pakistan, Constitutional Petitions 77 to 85/89.

Pakistan, it was held by the Supreme court of Pakistan that the right to access to information is prerequisite to the right to speech and expression. Similarly, it was also held by the supreme court of India that the right to life, liberty and speech also includes the freedom of information.

In 2010, the 18th amendment was adopted in constitution of Pakistan. Article 19-A was added into the constitution. This Article deals with freedom of information.[466] Now, the access to information is a constitutional right of the people of Pakistan. This right is an exception to the right to privacy. An information and data are accessed by the people as their fundamental right to safeguard public peace and national security. This Article provides the fundamental right of freedom to approach information to the citizens of Pakistan. This Article explicitly states that every citizen shall have the right to approach information related to the matters of public importance. However, this right is subject to reasonable restrictions enforced by law. This right is exercisable only in case of public importance. In this regard the Supreme Court said that the people in search of truth find rumours and speculations which leads towards the deterioration of society. The concealment of information results into the disruption of the country. Moreover, it shakes the confidence of public over the government.

Article 19-A is granted by the constitution and it is declared as the fundamental right of the citizens of Pakistan. It cannot be taken away or abridged by any law. In this Article a citizen of Pakistan is empowered enough to become independent o collect information from any public office as a matter of his right. This right is exercisable in case of public importance only. In this Article the institutions are not allowed to grab an information related to the affairs of public interest. The verdict of the Supreme Court further states that this right is not liable to be amended or curtailed.

---

[466] Article 19-A of Constitution of Pakistan, 1973.

People are entrusted with the right that they can access to the government to seek information relating to the public interest matters. Article 19-A is the fundamental right of citizens of Pakistan and it is enshrined in Chapter-II of the constitution of Pakistan, 1973.

A columnist while speaking about the Judgment of the Supreme Court gives his opinion. He says that the lawmakers have guaranteed the citizens of Pakistan with an unbridled right to access information. He further says that this right to freedom of information is guaranteed in the supreme law of the land so it cannot be alienated or taken away. Even the court has no authority to take away or curtail this right. It is the right of every person to access the information about government actions related to public affairs. Now such information cannot be preserved in the name of state or government.[467]

The verdict of the Supreme Court gave a great favour to the right to access to information. The freedom of information ordinance was there since 2002 but it was not incorporated in constitution of Pakistan. Therefore, it could not gain much importance till 18th amendment. But after this amendment freedom of information becomes the fundamental right. Now people can demand any record to be made public. They can inspect any public document whenever they require it. Moreover, they can challenge any public record if there is any inconsistency.

This is a great step to keep an eye on government and its functionaries. This is a good step towards transparency. People and government will work in more conducive environment. People may be able to know the functions of government in a better way. Along with all these blessings it is an intrusion into the privacy of others. The right to privacy is interfered by this right. This

[467] Majid Yar, *Cyber Crime and Society* (London: SAGE Publications Ltd, 2006): 49.

Article is a limitation upon the privacy of a person. Though the right to privacy of a person is not directly injured in this article. There may be a situation in which the right of an individual may be directly interfered under the umbrella of the said article 19-A. Therefore, it is suggested that there may be some amendment in this Article in which a balance may be maintained between the right to privacy and freedom of information.

The Local Government Ordinance, 2001

In this ordinance, there are also some provisions which allows the right to access information. In this ordinance the right to privacy is also limited by ensuring the right to access to information. In this ordinance the meetings of zila council are made public. It is stated in section 42 (7) that the meetings of the zila council shall be held in public and the people shall have the right to attend these meetings. Such meetings are directed to be held transparent. The policies and decisions taken in such meetings shall be made public. This is directed to make the public affairs in access of common man. It is also ensured so that misuse of power may be controlled. On the other hand, it is interference into the right to privacy. Sometimes, information may be critical or sensitive and it may be dangerous to share it with public.

Section 76 states that the information which has been gathered by conducting surveys shall be circulated by the Union Council Administration. Such information shall be circulated for public interest. But no option is provided for such circular. It is also not mentioned in this section that the information may be officially published or submitted in any office from where people may access it. This is also against right to privacy. Some information may be related to specific class, gender or culture which needs privacy. Moreover, it may be against public interest to make an information a part of public record.

Further, section 114 (4 and 5) of this ordinance state that the local government will provide the statement of accounts. This statement will be the part of public record. This statement will be displayed in some prominent place so that every person may have access to read it. But this is not practically followed by the union council's officials. Moreover, the accurate statemen is not prepared only factual documents are designed to fulfil the requirements of the ordinance. This is not infringement to right to privacy but it gives access to information related to the expenditures of a district administration. It is a limitation to the privacy of local government with regard to the statement of accounts.

Section 137 of the Ordinance says that every citizen has a right to access information of the public matters. This section further states that such matters also include the statement of accounts, details of expenditures, policies, initiatives and decisions taken by the local government. The local government administration is answerable to the general public for the matters of public interest. This section also entrusts a citizen to collect information about the officials of local government. Further the citizen is also capable of gathering knowledge about the efficiency and functions of such officials. Such information regarding the policies, decisions, official staff and their performance is required to be maintained in a register. Such register will be available to the public for the purpose of access to information. This section is interference with the right to privacy of officials. it can be misused against the local government officials. There must be reasonable restrictions on this unfettered right to access to information.

The provisions of the Local Government Ordinance, 2001 are needed to be balanced with regard to right to privacy and right to access to information. The public importance matters are needed to be accessed by the people but there may be some justified restrictions with regard to the

critical issues. Sometimes the open access to information made it more difficult to carry on certain government functions by officials. The common people may be unable to differentiate between the freedom of access to information and right to privacy. The District Ombudsman is appointed to remedied the aggrieved persons who are not entertained with desired information. However, breach to privacy is not discussed in this ordinance. Abuse of this right is also a drawback of this ordinance as a common man is not fully aware about the nature of information which is made available in it.

Investigation of Fair Trial Act, 2013[468]

The said Act was enacted in 2013 and it appeared to be a great danger to the privacy of individuals. A person's email, information, data, message, phone calls and computer or mobile based communication can be accessed upon a warrant of court. It is the clear infringement of constitutional right to privacy of an individual. However, the court shall issue warrant only in the condition of reasonable suspicion of the commission of a scheduled offence.[469] In *Jamat-i-Islami Pakistan v. Federation of Pakistan*, it was held by Supreme Court that the act of legislation having the force of law especially which deals with the social and financial aspects must be clear and free from burliness. Moreover, no mathematical or absolute precision is required but only a definite and certain legislation is needed. An enactment that is vague is the nullity.[470]

In *Pakistan Tobacco Co. Ltd. vs. Government of NWFP*, the Supreme Court of Pakistan held that the uncontrolled unguided and unbridled executive powers to the government official are unconstitutional. Further it is decided that the conduct of criminal is being charged and has been

[468] http://www.na.gov.pk/uploads/documents/1361943916_947.pdf (Last accessed: 20 November, 2018).
[469] Section 10 of an Investigation of fair trial Act, (2013).
[470] *PLD 2000 SC 111.*

made responsible for penalty must be defined clearly otherwise it would amount to be arbitrary.[471] In *Waris Mesah v. State* (PLD 1975 SC 157) it was decided by the supreme court the right of equality is not infringed only in the case of unguided and uncontrolled powers of executives but only in the situation of arbitrary use of such powers the said right is violated.[472] In *Mehram Ali v. Federation of Pakistan*[473], the Supreme Court strike down the provision of the Anti-Terrorist Act[474] by deciding that the officer must be empowered to make fire. In the light of above mentioned Judgments, the present Act is therefore needed to be amended to cater the objectives of this legislation as well as to bring it in line with the provisions of Constitution of Pakistan.

Pakistan Electronic Media Regulatory Authority (PEMRA)Ordinance, 2002

PEMRA Ordinance is also a limitation to the right to privacy of a person. The opening sentence of this ordinance is inserted with the intention to provide an access to information. It is stated in the starting phrase of this ordinance that this ordinance is adopted with the aim to improve the standards of information. The promise that is embodied in the preamble is the restraint to privacy of an individual, organization, institution, state and government. This provision is against the right to privacy and it must be invoked with great care and caution in order to protect the privacy.[475]

Article 05 of the ordinance invests the federal government with the power to issue directives to the PEMRA Authority. It is stated in Article 05 that the federal government may issue directive if it thinks that a certain issue comes within the ambit of a directive. Such power is exercised in the cases where the instructions of federal government are not followed or where the

---

[471] *Pakistan Tobacco Co. Ltd. vs. Government of NWFP, (PLD 2002 SC 460).*
[472] *Waris Mesah v. State*, (PLD 1975 SC 157).
[473] *Mehram Ali v. Federation of Pakistan. (PLD 1998 SC 1445).*
[474] Section 5 (2) (i) of Anti-Terrorism Act, (1997).
[475] Preamble to the "Pakistan Electronic Media Regulatory Authority, (PEMRA) Ordinance", (2002).

critical or sensitive matter of government or any institution is going to be broadcasted. If it comes into the knowledge of federal government that a certain act of government that will be liable to some unwanted results, is going to be published by a television channel, that may be ordered to be stopped. The PEMRA authority is also empowered to stop such program.

PEMRA Cable Television (Operations) Regulations, 2002 also impose limitations on the right to privacy by providing right to access to information. However, Articles 21 and 25 respectively impose some restrictions on this right to information. It is stated in Article 21 that the authority may restrict any service provider or cable operator to transmit any program or to broadcast any channel which is likely to spread hate speech or any other unwanted material. Moreover, if any channel is appeared to be against the maintenance of law it shall also be banned.[476]

Article 25 gives the penal consequences if someone contravenes the provisions of Article 21. It is stated that if a licensee or cable operator broadcast any channel which is against morality, law or public interest or liable to create hate speech then he shall be punished. The machinery shall also be forfeited and the building shall be taken into possession where such transmission was aired. These provisions are not the in favour of the right to privacy but only provides certain parameters to broadcast a program. However, the authority may consider any information as liable to be banned.

[476] Article 21, "The Pakistan Electronic Media Regulatory Authority Cable Television (Operations) Regulation", (2002).

Conclusion

From the above discussion it is concluded that the right to privacy is embedded in Pakistan's constitution and other legislations. It is the need of hour to implant this right to privacy in cyber legislation too. The examination of existing Pakistani legal framework highlighted the necessity of an appropriate cyber code. This cyber code should be sufficient enough to secure and protect the digital information and data of individuals in various corporate, government and other public or private sectors. In order to design an appropriate legal paradigm these government institutions and business sectors should work together. Though, Pakistan is striving to make better laws. It has adopted various international pacts and agreements. These instruments also favour the privacy as a basic human right. After making the acknowledgment of privacy as a fundamental right, it is also the duty of Pakistani lawmakers to adopt a such code of cyber laws which may be sufficient to protect the privacy of individuals on virtual world. Moreover, being the member of international community, Pakistan should also involve global cooperation to secure the privacy not only on state level but also on global level. It is suggested that Privacy Protection Act along with guidelines shall be adopted by parliament. This Act shall be designed after consultation with various stakeholders. The international regulations and principles shall also be considered while adopting this law. The last but not the least suggestion in this regard is that the certain prevailing laws must be amended to bring them in accordance with the said Privacy Protection Act. This Act shall repeal those provisions of other laws which seems to compromise the privacy. The next chapter is aimed to critically analysis the cyberspace laws and right to privacy in Pakistan.

Chapter Five

A Critical Analysis of Cyberspace Laws and Right to Privacy in Pakistan

Introduction

This chapter is aimed to provide a critical analysis of cyberspace laws, right to privacy and current trends of privacy issues in cyberspace with specific reference to Pakistan. This chapter examines the challenges which the government of Pakistan is facing to prevent the cybercrimes by keeping in view the breach of privacy in cyberspace and suggests a way forward to deal with this issue. A legal mechanism is required to curb the e-frauds in everyday life of individuals. In this context, this Chapter is divided into four Sections. Section one discusses the cases of breach of right to privacy in Pakistani society. It explains surveillance by state, foreign surveillance, surveillance on civil liberties, corporate espionage and threat to cyber security of Pakistan. Section two addresses the victimized sectors of cybercrimes. In this respect, it highlights banking sectors, email, software policy, social media, websites and internet. Section three critically analyses cyber legislation of Pakistan. It discusses the insufficiency of data protection laws in cyberspace and highlight the other relevant lacunas in cyber laws of Pakistan. Section four addresses the application and enforcement mechanism of privacy rights in Pakistan and considers it as a big challenge for Pakistan in terms of implementation of privacy laws. It also explains differences in the application of domestic and international human rights safeguards. Further, it argues that domestication of international laws pertaining to privacy in Pakistan is essential for protection of privacy rights.

5.1 Cases of Breach of Right to Privacy in Pakistani Society

With the advent of internet, 3G/4G technologies and ICTs Pakistan is making an effort to make advancements in both, public and private sectors. It is the need of the time to become updated in the field of digital technology as e-culture is mushrooming in country. The fast advancement of technology is a great danger for countries especially for the developing countries to protect the right to privacy not only of individuals and organizations but also for the country itself. The digital era has made it easy to interfere into the one's right to privacy. The government is needed to make such a legal system to combat the issue of intrusion into privacy.

The privacy, as it has already been discussed in chapter two, has various dimensions. These dimensions are related to the specific kinds of privacy. In this chapter the researcher is going to discuss the present concerns related to privacy of information and data in cyberspace. Various kinds of privacy breach will also be discussed. The common trends of infringement of privacy of an individual, an organization and state will be addressed. The situation of Pakistani society in the perspective of privacy apprehensions in the digital era are going to be analysed.

5.1.1 Surveillance by State

It is reported that the phone calls of the citizens are tapped on regular basis by the intelligence bodies and law enforcement agencies.[477] Such as the Inter-Services Intelligence (ISI), Intelligence Bureau (IB), Military Intelligence (MI) and the police are highlighted in these activities.[478] These

---

[477] Grare, Frédéric. *Reforming the Intelligence Agencies in Pakistan's Transitional Democracy*. Washington, DC: Carnegie Endowment for International Peace, 2009.

[478] Ibid;

calls are recorded without the permission of the citizens. In 2015, the IB and ISI revealed before the Supreme Court of Pakistan that they were monitoring and tapping nearly 6,000 and 7,000 phone lines every month respectively.[479] It was also requested by ISI to hear the 19 years old Suo moto case in close doors and in cameras. Phone calls surveillance by state intelligence agencies are also the breach of privacy rights.[480]

Farooq Ahmed Khan Leghari (Late), the former President of Pakistan, claimed that the late Benazir Bhutto's second government was dismissed in the result of phone tapping[481]. The women members of the National Assembly also complained many times in the past for the surveillance of their phone calls.[482] National Database and Registration Authority (NADRA) is one of the major biometric and centralized databases of the globe for the identity cards of the citizens of Pakistan.[483] It has experienced much mismanagement along with data privacy breaches[484], fake registration of ID cards[485] and corruption by official of NADRA[486]. This is a threat to the privacy of individuals[487]

---

[479] The Express Tribune. "Over 5,000 phones being tapped by IB, SC told". (2015). Online available at: https://tribune.com.pk/story/890074/over-5000-phones-being-tapped-by-ib-sc-told/ (Last accessed: 16 November, 2018).

[480] Nathan McAlone, "The 15 Companies That Flooded Your Inbox with the Most Email Spam in 2015," Business Insider, (2016).

[481] Ibid;

[482] KD Citron, H. and Norton, "Intermediaries and hate speech: Fostering digital citizenship for our information age". *Boston University Law Review*, Vol. 91, (2011): 1435–84.

[483] Report of ProPakistani, "NADRA Has Issued 101 Million ID Cards, Blocked 125K Fake Cards, (2016). https://propakistani.pk/2015/11/26/nadra-has-issued-101-million-id-cards-blocked-125k-fake-cards/ (Last accessed: 16 November, 2018).

[484] Pakistan Today. "SBP looking into NADRA-MasterCard agreement over concerns of possible breach of security of national database", (2017). http:// profit.pakistantoday.com.pk/2017/01/26/sbp-looking-into-nadra-mastercard-agreement-over-concerns-of-possible-breach-of-security-of-national-database/ (Last accessed: 16 November, 2018).

[485] The Dawn, "FIA to go after 'corrupt' Nadra officials", (2015). https://www.dawn. com/news/1180042 (Last accessed: 16 November, 2018).

[486] PakWired, "How Secure Are NADRA's Critical Information Systems?". (2016). https://pakwired.com/how-secure-are-nadras-critical-information-systems/ (Last accessed: 16 November, 2018).

[487] Bytes For All, Pakistan. "RTI Requests - National Database and Registration Authority (NADRA)". (2016). http://rtirequests.pk/subject-of-rti-request-national-database-and-registration-authority-nadra/ (Last accessed: 16 November, 2018).

and a damage of trust over government. It is also surprising that the NADRA has refused and shut down its whistleblower program. The promise of accountability and fairness could not be meet because of this setback.[488]

In Pakistan, the government is going to introduce a "Safe City project". Under this project, high-powered cameras are going to be installed in Islamabad and other cities of Pakistan. This project is designed with the cooperation of NADRA and Huawei. The biometric databases from NADRA shall be connected to these cameras. These cameras are connected to the National Database and Registration Authority (NADRA). Punjab, Sindh and KPK are also inclined to fix CCTV cameras in their territories. High powered cameras are implanted in Islamabad. These high resolution cameras are designed on the advanced technologies. About 1900 cameras of high technology with the power of facial recognition have been fixed in Islamabad. These 32-megapixel cameras have also the ability to use global positioning system (GPS) to follow the people and their Subscriber Identity Module (SIM) as well as International Mobile Equipment Identity (IMEI) codes. Such installation of cameras is the digital surveillance of people and which allows the government to trace the people without their consent. Digital surveillance is also an interference with right to privacy.[489]

A report of Citizen Lab, revealed that various intrusion tools are used by different servers in Pakistan. These tools are used to collect the information from a remote computer system. The

---

[488] Report of ProPakistani, NADRA Shuts Down Its Whistleblower Program, (2016). https://propakistani.pk/2016/04/13/nadra-shuts-down-its-whistleblower-programme/ (Last accessed: 16 November, 2018).

[489] Ahmad, Mahvish, and Rabia Mehmood. "Surveillance, Authoritarianism and 'Imperial Effects' in Pakistan." *Surveillance & Society* 15, no. 3/4 (2017): 506-513.

passwords are also cracked with the help of these tools.[490] Sometimes the data is damaged by using malware. Moreover, a direct access is gained over others webcams and cell phones with the help of these dangerous intrusion trojans. It is exposed by different evidences, the report of Citizen Labs and the information shared by a hacker named, Phineasfisher, that the advanced surveillance has been made with the help of spywares.[491] These spywares include FinSpy, FinUSB and FinIntrusion Kit usually called FinFisher,[492] which are used for advanced monitoring and observation. [493]This spyware has also been licenced in Pakistan as well as working on a government-owned server, Pakistan Telecommunication Limited (PTCL). [494]This spyware is excellent to reach to a private information and data. It is also able to hack public Wifi networks. Bytes for All (B4A) Pakistan,[495] have moved a petition on the basis of public interest to the Lahore Hight Court. This petition was made to answer the question for the use of this malicious spyware which however is not decided

---

[490] Dahan, Michael. "Hacking for the homeland: Patriotic hackers versus hacktivists." In *ICIW 2013 Proceedings of the 8th International Conference on Information Warfare and Security: ICIW 2013*, p. 51. Academic Conferences Limited, 2013.

[491] Spyware is a type of malicious software -- or malware -- that is installed on a computing device without the end user's knowledge. It invades the device, steals sensitive information and internet usage data, and relays it to advertisers, data firms or external users.

[492] FinFisher or FinSpy is a piece of computer spyware designed to allow someone to spy on a computer or mobile phone. FinSpy is a commercial spyware. FinSpy is spyware for Android, iOS, Windows, macOS, and Linux that is sold legally.

[493] Prashant Mali, *A Text Book of Cybercrime and Penalties* (Indiana: Repressed Publishing LLC, 2006), 3.

[494] The Dawn, "Customer 32 — who used FinFisher to spy in Pakistan?", (2014). https://www.dawn.com/news/1127405. (Last accessed: 16 November, 2018).

[495] Bytes for All (B4A), Pakistan is a human rights organization and a research think tank with a focus on Information and Communication Technologies (ICTs).

yet.[496] It is also observed that Pakistan has also make the interaction with hacking experts to gain a tool capable of having access to remote Control systems.[497]

5.1.2 Foreign Surveillance

Pakistan has acted as a third-party partner to cooperate with United States' National Security Agency (NSA). It was exposed by Edward Snowden who was a contractor with US Government and became a whistle-blower. He stated that being the third-party partner Pakistan provides the opportunity of a mass surveillance in Pakistan. He revealed that Pakistan permitted NSA to connect surveillance equipment with its fiber-optic cables and a covert RAMPART-A[498] Surveillance Program to observe the people on internet and cyberspace.[499] "Privacy international" also talked about the cooperation between the Government of Pakistan and NSA for the intelligence sharing arrangements and understandings.[500] Such acts of Government are the violation of right to privacy of the Pakistani peoples. The report exposed the fact that the NSA regulates its services at U.S. embassy and Consulates in Pakistan for the collection of information and data. NSA and U.K. Government Communications Headquarters (GCHQ) also shared the element that the Pakistan is working as third party under a Signal Intelligence (SIGINT) to provide surveillance facilities to US NSA.[501]

---

[496] Bytes for All. Pakistan. "Loss of privacy is always permanent - Snags in hearing of FinFisher case at Lahore High Court", (2014). http://content.bytesforall.pk/node/143. (Last accessed: 16 November, 2018).
[497] The Dawn. "Hacking Team hacked: The Pakistan connection. and India's expansion plan", (2015). https://www.dawn.com/news/1196767. (Last accessed: 16 November, 2018).

[498] RAMPART-A is the code name for global mass surveillance and world-wide signals intelligence partnership program led by the United States National Security Agency (NSA). Aim of the program is to "gain access to high-capacity international fiber-optic cables that transit at major congestion points around the world".

[499] Prashant Mali, *A Text Book of Cybercrime and Penalties.* Indiana: Repressed Publishing LLC, (2006), 3.
[500] Debarati Halder and K. Jaishankar. *Cyber Crime and the Victimization of Women: Laws. Rights and Regulations (*Hershey: Information Science Reference, 2012), 15.
[501] Ibid;

Pakistan's ISI agency also worked with NSA and UK's Government Communication Headquarter (GCHQ) to accomplish the task of installing some surveillance programs. SKYNET[502] and Fairview programs are reported to be implanted in Pakistan computer networks to monitor and collect the information and data.[503] SKYNET program is utilized to abstract the required information of a person by applying it scientifically to a flawed algorithm. It is reported that the SKYNET collected the cellular information and metadata[504] of about 55 million people from Pakistani networks.[505] This metadata was implemented to an illogical and vague algorithm to collect and trace the information about terrorists to make drone attacks. This algorithm used to gather information from the metadata of about 80 properties to ascertain the personality traits of a person who would be likely to become a terrorist. These properties are associated with the metadata of a person's information shared with different networks and institutions at the time of various transactions and cyber activities.

Ahmad Muaffaq Zaidan, an investigative journalist and the bureau chief of Islamabad Al Jazeera's Islamabad was erroneously considered the member of "Al Qaida". Under this wrong

---

[502] SKYNET is a program by the U.S. National Security Agency that performs machine learning analysis on communications data to extract information about possible terror suspects. The tool is used to identify targets, such as al-Qaeda couriers, who move between GSM cellular networks.

[503] The Hindu News (Newspaper) "Pakistan has built a massive surveillance state: Report". (2015). http://www.thehindu.com/news/international/south-asia/pakistan-has-built-a-massive-surveillance-state-report/article7402062.ece (Last accessed: 16 November, 2018).

[504] Metadata · It describes relevant information about the data. It is always informative. It is always processed. It is stored inside a data dictionary.

[505] Arstechnica UK. "The NSA's SKYNET program may be killing thousands of innocent people". (2016). https://arstechnica.co.uk/security/2016/02/ the-nsas-skynet-program-may-be-killing-thousands-of-innocent-people/ (Last accessed: 16 November, 2018).

perception he was kept under surveillance and observation for terrorist activities.[506] NSA put his name in the "terror watchlist" which was made by the agency on the sources of information drawn by metadata. Faisal Gill is another name which was mentioned on the surveillance goals of NSA and FBI.[507] Although he was appointed after a secret security clearance in the department of homeland security in the regime of George W. Bush. These practices of surveillance are a great danger to freedom and liberty of peoples of Pakistan. It also amounts the breach of privacy and security of persons and their information.

On 5th June 2013, it was reported by a British newspaper, Guardian, published the revelations made by Edward Snowden. He was the employee of the US National Security Agency (NSA). He acted as the whistleblower and revealed that the NSA and the UK's Government Communications Headquarters (GCHQ) conducted the global surveillance. He made these statements on the basis of available evidence and proof of communication surveillance.[508] According to the revelation the NSA was monitoring and collecting the telephones tapping of millions of people from the worldwide. The Washington post[509] and the Guardian[510] newspaper also exposed that the nine internet firms are directly involved into recording and tapping of

---

[506] Cora Currier, Glenn Greenwald, and Andrew Fishman, "US government designated prominent Al Jazeera journalist as member of Al Qaeda", The Intercept, 8 May, (2015). Online available at: https://firstlook.org/theintercept/2015/05/08/u-s-government-designated-prominent-al-jazeera-journalist-al-qaeda-member-put-watch-list/ (Last accessed: 16 November, 2018).

[507] Glenn Greenwald and Murtaza Hussain, "Meet the Muslim American Leader the FBI and NSA Have Been Spying On", The Intercept, 9 July 2014, online at: https://firstlook.org/theintercept/2014/07/09/under-surveillance/ (accessed 28 May 2015)

[508] Ben Emmerson QC, "the UN Special Rapporteur on counter-terrorism and human rights, two years after Snowden: protecting human rights in an age of mass surveillance".

[509] The Washington Post, "Here's everything we know about PRISM to date", (2013).https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prismto- date/?utm_term=.d034810205c1 (Last accessed: 16 November, 2018).

[510] KD Citron, H. and Norton. "Intermediaries and hate speech: Fostering digital citizenship for our information age", *Boston University Law Review*, Vol. 91, (2011), 1435–84.

communications of individuals by NSA. These internet firms include the Facebook, Google, Microsoft and Yahoo. The communication was tracked with the help of a special programme known as "PRISM".[511]

The only legislation, PECA (2016), was adopted to curb the cyber-crimes and to regulate the cyberspace.[512] PECA, 2016 allows the state to transfer the data to foreign government and agencies. It also authorizes the PTA and other investigating agency to access the data and to seize such data and devices without the warrant of court.[513] The provisions of PECA, 2016 also encourage the state to intervene into the privacy of individuals and to retain data up to one year.[514] Anonymity[515] is also made impossible by decryption of an information and data.[516] Further, this Act also authorises the investigation agency and PTA to approach and access the traffic data and information about telecommunication subscribers. It also authorizes the PTA and investigation agency to seize the traffic data and the device on which such data is operated without the warrant of the court.[517] This Act permits the cooperation with foreign governments, organizations and agencies to transfer the required intelligence information. No prior permission from the court is required to make such sharing of information. The description of data and information is also

---

[511] PRISM is a code name for a program under which the United States National Security Agency (NSA) collects internet communications from various U.S. internet companies.

[512] The Prevention of Electronic Crimes Act (PECA), (2016) (Act No.XL of 2016).
[513] Section 32 of PECA, (2016).
[514] Ibid; Section 29.

[515] Anonymity describes situations where the acting person's identity is unknown.

[516] Ibid; Section 35.
[517] Ibid; Section 30.

allowed to hinder the anonymity by persons.[518] Encryption[519] and anonymity are the necessary techniques to shield the information and privacy of a data along with its belongings to someone in cyberspace.[520] This Act is also against the international provisions of privacy when it allows the service providers to retain the traffic data of users for one year.[521] These provisions of PECA, 2016 are in contradiction to the right of privacy without the clear laws dealing with data retention.[522]

In terms of religious expression, the Law Enforcement Agencies (LEAs) raised their surveillance and monitoring on the expression of religious beliefs on internet. This resulted from an order of Islamabad High Court (IHC) in 2017, when it authorized the Interior Ministry (IM) and PTA to remove the blasphemous contents from internet and to block its approach on social media.[523] The IHC ordered to put the names of the persons who committed the blasphemy into the exit control list.[524] In the result of this order the FIA sanctioned the surveillance of public in regard to the blasphemous contents and make it possible on social media to report about such contents. It is also not difficult to hack one's account and misuse it for making posts and spread material which amounts to religious beliefs of one's sect or religion. There are no explicit measures provided for

---

[518] Ibid; Section 32.

[519] Encryption is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called cryptography.

[520] David Kaye, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", A/HRC/29/32, (2015).

[521] Section 29 of PECA, (2016).

[522] Haroon Baloch, "Internet Rights and Legislation in Pakistan: A Critique on Cyber Crime Bill 2016". http://www. net freedom. pk/ wp- content/ uploads/2016/06/CSO- criticism- on- PECB-2016_IssuePaper (Last accessed: 16 November, 2018).

[523] The Express Tribune. "Blasphemy: IHC directs authorities to block all social media if necessary". (2017). https://tribune.com.pk/story/1348784/ ihc-directs-authorities-block-social-media-necessary/ (Last accessed: 16 November, 2018).

[524] The Nation. "Put blasphemers on Exit Control List,' IHC tells govt". (2017). http: nation com.pk national 08-Mar-2017/put-blasphemers-on-exit-control-list-ihc-tells-govt (Last accessed: 16 November, 2018).

the interpretation of blasphemy according to unanimous consensus of all Islamic Sects.[525] Blasphemy is being used as a weapon against religious monitories and liberal persons for personal interests.[526]

5.1.3 Surveillance on Civil Liberties

It is reported by internet rights activists that the people feel discomfort from being regularly monitored by the state.[527] The accelerated surveillance impairs the activities and ability of persons to live free and work with devotions. The sense of observation creates the fear of continuous monitoring by a state and the accessing of information or data produces the danger of damage to them or their information. It is also observed that the prohibition of encryption resulted into misuse of information.[528] An activist for minorities' rights was intruded by LEAs directing him to not leave his residence or to switch off his cell phone containing a particular number. This resulted into the ending of his project and removal from his organization because of aggravated surveillance.[529]

The liberal and progressive-minded persons from academic circles, religious groups, political masses and literary circles are targeted for close surveillance. It has become the reason to challenge the government. Legislations, policies, religious grouping and political movements in a

---

[525] The Nation, "Pakistani right cries 'blasphemy' to muzzle progressives", (2017). http://nation.com.pk/national/17-Jan-2017/pakistani-right-cries-blasphemy-to-muzzle-progressives (Last accessed: 16 November, 2018).

[526] Independent. "Pakistan blasphemy laws increasingly misused to settle petty disputes against Christians", (2012). https://www.independent.co.uk/ news/world/asia/pakistan-blasphemy-laws-increasingly-misused-to-settle-petty-disputes-against-christians-a6768546.html (Last accessed: 16 November, 2018).

[527] Ahmad, Mahvish, and Rabia Mehmood. "Surveillance, Authoritarianism and 'Imperial Effects' in Pakistan." *Surveillance & Society* 15, no. 3/4 (2017): 506-513.

[528] Farid, Shahid, M. Alam, G. Qaiser, A. A. U. Haq, and J. Itmazi. "Security threats and measures in E-learning in Pakistan: A review." *Tech J* 22, no. 3 (2017): 98-107.

[529] PTA, "Directive No.17-1/2010/ Enf/PTA(VPN). PTA's Monitoring and Reconciliation of Telephony Traffic Regulations", (2010).

society are the most common concerns. It has also put in danger the literary, intellectual, religious and democratic circles of a state.[530] Most of the times such observation and monitoring is used to get some ulterior motives and personal interests under the disguise of religion or politics. Like, a Christian boy was charged with the offence of blasphemy for making a like to the post shared to him on his Facebook account[531]. Journalists, bloggers, members of civil society and human rights activists are mostly targeted for their liberal approach on social media.[532]

In another instance five individuals; Salman Haider[533], Waqas Goraya[534], Aasim Saeed[535], Ahmed Raza Naseer[536] and Samar Abbas[537], were abducted in the offence for regulating and operating a controversial page on social media. Hatred remarks were passed on the social media against them on a page maintained by nationalists. Many religious, sexual, political and gender masses are involved into the online activities relating to the expression of beliefs. However, the practice of anonymity in cyberspace encouraged these groups to share their debates and to participate into the world of networks. But the raised level of surveillance and monitoring has put them into the fear of self-censor and to become the prey of targeted attacks for their views and ideas.

Right to privacy is also necessary for the equality of gender. It is observed and argued by the gender rights activists that the gender equality may be attained by providing a complete privacy

---

[530] Peter Jacob & Sunil Malik, Personal Interview, Center for Social Justice (CSJ) Lahore, (2017).
[531] Hassan Karrar, Personal Interview, Lahore University of Management Sciences (LUMS), (2017).
[532] Rabia Mehmood, Personal Interview, (Mar 2017). Lahore
[533] Salman Haider, "Front Line Defenders", (2017). https://www.frontlinedefenders.org/en/profile/salman-haider (Last accessed: 16 November, 2018).
[534] Ibid;
[535] Majid Yar, *Cyber Crime and Society* (London: SAGE Publications Ltd, 2006), 9.
[536] Ahmed Raza Naseer, "Front Line Defenders", https://www.frontlinedefenders.org/en/profile/ahmed-raza-naseer (Last accessed: 16 November, 2018).
[537] Samar Abbas, "Front Line Defenders", (2017). https://www.frontlinedefenders.org/en/profile/samar-abbas (Last accessed: 16 November, 2018).

to the personal information to all persons without discrimination of sex. Women, young girls and children are more wanted for the criminals to infringe their privacy and to harass them on social networks. The private information including pictures, tapping of calls and videos are commonly used to harm the victim. Such victimization and encroachment into privacy mostly harm the person and his or her family in the long term of the time. Character assassination, societal discrimination, workplace harassment, sex shaming, physical harm, forced sexual relations, unwanted marriages, honour killing, child marriage and child pornography may be the consequences of this gender discrimination.

Instances of sexual abuse, suicide and murder are the frequent reaction in Pakistani society towards breach of personal information belonging to a female. Making pictures, video, recording of audio calls, and misuse of shared communications are the illustrations of breach of privacy in respect to a specific person. If such person is the girl or woman then its results will be bitterer for the victim, her family and society. Females are the common and frequent prey of mala fide brains to make them the quarry of their lust. On the other side, these females are not supported by their own families and brutally beaten or murdered or stigmatized in the society. A social media celebrity was slaughtered because of the disclosure of her personal information.[538] However, in other cases the men are also targeted for these practices.

Many rural and urban areas of the Pakistan are far behind in the matters of freedom and liberty of women. The taboo of family honour and respect is traditionally linked only with the females of the family especially in rural areas. The females are restricted from their genuine needs like education, employment and other upbringings on the pretext that these things are against the

[538] Bytes for All, "Gender Tech & Privacy Event", (Feb 17, 2016).

honour and a source of shame for whole members of family or society. 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.[539] On another occasion, five women were brutally murdered among of them one was the minor. The reason behind the killing was a video of a singing and clapping in a group of girls on the eve of a marriage and this video went public by sharing on social media.[540]

In addition to these instances of conservative cultures, there is also illustration of such anti feminism activities in well developed areas of Pakistan. Many women had complained for undue and obsessed surveillance. In other cases, the women are also charged with the offence of blasphemy, anti-state practices or liberal conduct by well organized groups dealing with online activities. The discussion and expressions shared on social media are made target for this discrimination again these women.[541]

Children are also more vulnerable group of Pakistani society to become target of sexual violence and forced marriages. For avoiding minor's sexual violence, it is necessary to protect children and their privacy, safeguards may be implemented in an effective manner. The reports revealed that the worst child abuse scandal was happened in Kasur, Punjab in which approximately 280 children were sexually abused on camera.[542] Later on, the families of such children were also targeted and disturbed. These children and their families were blackmailed.[543]

---

[539] Ibid;

[540] Majid Yar, *Cyber Crime and Society* (London: SAGE Publications Ltd, 2006), 78.

[541] The Express Tribune, "Chilas town: Saving 'honour' or family riche", (2017). https://tribune.com.pk/story/576737/chilas-town-saving-honour-or-family-riches (Last accessed: 16 November, 2018).

[542] BBC News, "Pakistan child sex abuse: Seven arrested in Punjab", (2015). http://www.bbc.com/news/world-asia-33843765 (Last accessed: 16 November, 2018).

[543] The Express Tribune, "Kohistan 'honour' killing: Four years on, no justice in sight", (2016). https://tribune.com.pk/story/1034553/kohistan-honour-killing-four-years-on-no-justice-in-sight/ (Last accessed: 16 November, 2018).

Similarly, a group of child abuse was also reported in swat, Khyber Pakhtunkhwa which was involved for having forced sex with children on camera.[544] Another case of similar nature was also reported from South Punjab. In this case a girl was blackmailed and rapped by a group of persons for a period of months. This girl was filmed secretly by these culprits while having sex with her paramour.[545] Later on, she was blackmailed and forced to make relation with other men.

These instances of privacy violation are very common in our country. Privacy intrusion results into many problems in a society. The personal information of people has become public and causes injury to the reputations of them. A boy of 16 years old sexually abused a minor girl on camera in Khyber Pakhtunkhwa. After this sexual assault the boy shared the pictures on social media and other offline networks. However, in the consequence of this incident he was also punished for imprisonment.[546]

The violations of privacy are needed to be addressed at national level. States should make such laws as to protect their citizens from every type of privacy violation. In this respect there should also the proper implementation of laws for the protection of children's right. Special measures may be taken to tackle this issue. Pakistan is also among those countries which has ratified the convention on the rights of the child. The optional protocol to the convention on the rights of the child has been adopted by Pakistan to protect the child abuse.[547]

---

[544] Daily Pakistan. "Another organized child abuse ring discovered in Pakistan. hundreds of photos and videos recovered", (2016). https://en.dailypakistan.com.pk/headline/organized-child-abuse-rings-khyber-pakhtunkhwa/ (Last accessed: 16 November, 2018).

[545] Bytes for All. Pakistan. "Case Studies - Technology Driven Violence Against Women". (2014). http://content.bytesforall.pk/CaseStudies-TechnologyDrivenViolenceAgainstWomen (Last accessed: 16 November, 2018).

[546] The Dawn. "First child convicted in KP of pornography". (2013). https://www.dawn.com/news/1031509 (Last accessed: 16 November, 2018).

[547] "Report of the UN OHCHR", Online available and retrieved from: http://tbinternet.ohchr.org/_layouts/TreatyBodyExternal/Treaty.aspx?CountryID=131&Lang=EN (Last accessed: 16 November, 2018).

These measures may be specifically implemented to curb the curse of child pornography, child prostitution and the sale of children. It is the responsibility of a state to protect the privacy of its minors so that the children and their families may be secured from extortion. The privacy of children should be protected in all aspects to save them from every harm and destruction. Because of such abuses and traumas, the personality of a child becomes destructive. It's the obligation of a state to preserve the children as an asset of the future. Moreover, such type of privacy danger is the sign of weak administration of justice in a society.

Social media is a safe place for sexual minorities.[548] The sexually persecuted group feels more secure on online association. They feel free to associate with the people of their interest. Online applications provide much room for anonymity. It also protects people from being abused physically. However, the reports revealed that such persons are more vulnerable after the sharing of their identity on social media. Many of them are reported to become a prey of murder after disclosure of their identifications on mobile dating applications and other social media.[549] Such activities must be controlled by implementing adequate legislation.

It is also reported that peoples belonging to sexual minorities were shared on Instagram accounts. Their personal pictures were also uploaded on this account. This account was administered by unknown persons and 250 persons were victimized by this act. It is the gross violation of privacy right as no consent was taken from the individuals before making their

---

[548] Rafi, Muhammad Shaban. "Cyberbullying in Pakistan: Positioning the aggressor, victim, and bystander." *Pakistan Journal of Psychological Research* (2019): 601-620.

[549] The New York Times, "Pakistani Says He Killed 3, Using Gay Site to Lure Them", (2014). https://www.nytimes.com/2014/04/29/world/asia/pakistani-man-confesses-to-using-gay-sites-to-lure-victims.html?_r=0 (Last accessed: 16 November, 2018).

personal life public. Such pictures were collected from various mobile data applications. However, this account was blocked and deleted from Instagram after protest of some activists.

5.1.4 Corporate Espionage

Corporate espionage is the collection of information about the business of a corporation. It may be related to the marketing ideas of a business company. This information may be about the financial sources, bids, salaries, stockholders, corporate strategies, business methods, customers dealings techniques and the staff of the corporation. The said information may be collected to compete a business rivalry or to damage the information system of the company.

Corporate espionage is a global trend and it requires some special expertise to do it. Intelligence and engineering skills are required to monitor the record of a company. The most common skills include phone tapping, websites hacking, dumpster diving, network leakage, and cryptography. The surveillance is performed to injure the corporates in various aspects. It may cause financial loss to a company. It may result into customers loss. It maty cause defame of an institution. It may create public distrust upon a company. In some ways it may be performed to copy the products and marketing strategies of a business corporation.

Corporations are the dependents on computer networks. The economy is relying on different infrastructures designed by business companies. Government activities, business transactions, financial transfers, infrastructure activities are carried on computer networks. The corporations are vulnerable to the targets of hacking and espionage.[550] The competitors and foes encroach the critical infrastructure and information of corporation to destroy them. These attacks may be made from any part of the world. International organizations and hackers may also be

[550] David Wall, *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge: Polity, (2007).

involved to cause destruction to the economy of the country. Usually, the institutions' records and secrets are gained by some malicious software. Sometimes the skilled persons are hired to collect the business information. The cyber world and its related crimes have no territorial barriers, and this makes everything complex because evidence is very hard to come by. As global companies and governments join e-market places and business becomes borderless, their vulnerability multiplies. Privacy in these e-markets would be a major area of concern in the coming days, with greater degree of damages. What is of far greater serious concern is that cyber worms can turn everything upside down alone with a laptop as his weapon sitting in a basement or in a bathroom connecting it with a mobile phone and damages can take place in a matter of a few seconds.

The corporations should take strict measures to protect their name and fame. Experts should be hired to watch the security and protection of data. There must be practical approach to make the spying impossible. Latest technologies and software should be tried to defeat the intrusion attacks.[551] Networks and systems should be continuously monitored for any unwanted attacks. Employees should also be trained to combat these threats and to secure data on computer networks. Corporations are the backbone of economy and state should also help them to be protected and undefective.

It is also reported that the state institutions are involved into the surveillance of individuals and organizations. The digital communications of different business entities, individuals and organizations are monitored without the consent of the object. State institutions perform these observations with the help of advanced technologies acquired from national and international companies. Alcatel, Ericsson, Huawei, SS8, and Utimaco are the reported companies which are

[551] Report of EC, *Investigating Network Intrusions and Cyber crime*,:New York: EC-Council, (2010), 265.

providing the services of mass surveillances. Moreover, no transparent, judicial as well as legislative measures are adopted to do such surveillance.[552]

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. Such type of threat is a great danger for developing countries which are not sufficient in information technologies. It is the threat for the whole region as well. Strong policy measures should be adopted to combat it collectively.

It is also reported that the government is also provided with personal and desired information of institutions and individuals by internet servers including Facebook[553] and Google.[554] No adequate and satisfactory answer is given for the request and cooperation of such information. The deficiency of transparency is a serious concern for the internet uses of the country. It is the point of thinking that the telecommunication companies owned by Pakistan government are mostly working with the international corporations which do not provide the adequate standards for the protection of privacy and security of information shared through their channel. It is also the debate of the hour that the privacy policies which are designed for the collection, retention or transfer of data and personal information are gloomy and foggy which curtail many aspects of the privacy under the quilt of necessary and required information.[555]

---

[552] Privacy International, "Tipping the Scales: Security and Surveillance in Pakistan", (2015). https://www.privacyinternational.org/?q=node/624 (Last accessed: 16 November, 2018).

[553] "Facebook Transparency Report", (2012 – 2016). https://govtrequests.facebook.com/country/Pakistan/2016-H1 (Last accessed: 16 November, 2018).

[554] "Google Transparency Report", (2012 – 2016). Online available and retrieved from: https://www.google.com/transparencyreport/userdatarequests/PK/ (Last accessed: 16 November, 2018).

[555] The Dawn, "Pakistani telecoms' murky policies put users' privacy at risk: report", (2016). https://www.dawn.com/news/1305364 (Last accessed: 16 November, 2018).

5.1.5 Threat to Cyber Security of Pakistan

The geopolitical position of Pakistan and the anti-terrorism activities have invited many foreign governments to fund for advanced and sophisticated surveillance in Pakistan. Foreign surveillance is intrusive and advanced to counter insurgency and Islamist practices which made the privacy of a person more vulnerable. This interference of foreign agencies also required the Pakistan military to develop an innovative Communications surveillance Infrastructure. It made the surveillance more active in the country. Moreover, the sporadic targets of insurgency such as the Peshawar School attack by Taliban affiliated groups extended the surveillance practices.[556] Intelligence agencies are also conducting the intelligence functions by collection and using intercepted data and information. Pakistan armed forces have their own intelligence for each branch. Similarly, many other intelligence agencies like ISI, Joint signals Intelligence, Joint Intelligence Technical, Joint Intelligence X units and the FIA are interfering with information and communications for assigned tasks. Intelligence Bureau is also collecting intercepted data. Mass automated interception has been designed to intercept the communications of citizens under the cover of security concerns.[557] SIM cards are used to be registered.[558] These SIM cards are verified by the NADRA database.[559] Biometric system is also used to register these SIM cards with the help of fingerprints.[560] NADRA is reported as the largest database which contain almost 96% of

---

[556] The Dawn. "After Peshawar: Reassessing the terror threat", 18 December. (2014). http www. dawn.com/news/1151616 (Last accessed: 16 November, 2018).

[557] Report of Privacy International (2015), Tipping the Scales: surveillance and security in Pakistan. Available: https: www.privacyinternational org sites default files PAKISTAN%20REPORT%20HIGH%20RES%2020150722 0.pdf (Last accessed: 16 November, 2018).

[558] "Pakistani SIM users given until 17 May to register". Telegeography, 27 April, (2011), https www.telegeography. com/products/commsupdate/articles/2011/04/27/pakistani-sim-users-given-until-17-may-to-register/ (Last accessed: 16 November, 2018).

[559] Ibid;

[560] Ghulam Muhammad Kundi, Jacques Andre Bartoli and Serge Bail, *E-local government: Implementation barriers in Pakistan*, Lap-Lambert Academic Publishing, Germany, (2012).

data registration records of the persons. This record is easily accessible from the website of NADRA. Like, these ID cards and Smart National Identity Cards (SNIC)[561] are equipped with certain information including the name, address and family tree of the owner. These id cards are needed to acquire the various services in the country. These cards are used to open the bank accounts, to make travels, to purchase goods or any property, to apply for a job and to get health services. These types of transaction are usually held on ICTs. In this situation, these cards are the most vulnerable to crimes[562], frauds, forgery and misidentification or identity theft activities.[563]

With the advent of ICTs technologies new ways of threat are born. Cyberspace is the creation of advanced technologies. With the evolution of cyberspace, the non-traditional crimes also came into existence. These non-traditional crimes are a threat for the security of a country. This threat is different from the threats to the conventional territories of a state. Even this threat is entered into every aspect of the safety including air, water and space. This threat is commonly known as cyber warfare. Cyber warfare is a threat to the cyberspace of a nation. This warfare is borderless and transnational. States have shifted there each segment of business on cyberspace which is an easy target for the criminals to threat. Similarly, with the help of advanced technologies it is possible for the hackers to intrude into the important affairs of countries.

Pakistan has also shifted from the conventional courses of business to the digital technologies. The government, military, education, health and economy sectors are transferred to the ICTs. The critical infrastructures and sensitive information are implanted in cyberspace.

---

[561] Report of NADRA, "Solutions", (2015), https://www.nadra.gov.pk/index.php solutions (Last accessed: 16 November, 2018).
[562] Muhammad Azam Khan, "The information age and Pakistan", *Criterion*, (2013).
[563] Ibid;

However, the cyberspace is not much secured as it should be to protect the privacy and security of a state. Cyber warfare is the threat for the security of state. Pakistan is not fully secured from this threat. As it does not have enough security measures to control the access of the criminals in cyberspace. Pakistan is a developing country and lag behind in the cyber security. Occasionally it faces the issues of cyber-crime at public and private sectors. The major security concern of Pakistan are the financial institutions, critical infrastructures, and defense mechanism of military sectors.

Cyber warfare is also a permanent danger for Pakistan. All important websites of the Government contain necessary information or provide services to the public. Indian hackers accessed the Pakistani websites and deface these websites to harm the information and public trust. Similarly, websites of public and private corporations are hacked by criminals to gain their objectives. Pakistan should try to make cyberspace secure for the sake of its sovereignty. Cyber dependency has opened the new doors for security threats. Digital vulnerability of Pakistan websites experienced many times warfare attacks from national and international hackers. Terrorist organizations also attack the cyberspace to collect or destroy data. Sometimes, terrorist threat the Government to satisfy their demands or to make revenges.

Digital technology reliance has also affected the defense strategies of a state in the same way as other spheres of life. States have shifted to digital defense technologies. Cyberspace is not secured from danger to these technologies as well.[564] The critical infrastructures and important defense strategies are liable to intrusion because of transborder nature of cybercrime. The worst episode of this threat was the attack on Iran by U.S and Israel. The digital weapon known as Digital

[564] Naureen, Adeela, and Umar Waqar, "Indo Pakistan cyber war: Reality check." *The Nation*, 28 August, (2012).

Missal was used to destroy the nuclear system of Iran. This horrible missal was attacked with the help of Stuxnet virus. This virus not only destroyed the information but also the system as well. Such type of warfare is a permanent danger for the sovereignty of a state. Pakistan has also its nuclear system. There must be strong defensive techniques to protect the cyberspace. Cyberspace of Pakistan is also affected and targeted in propagandas against Islam and nuclear system of the country. According to a report Israel is trying to wage digital war against Islam and nuclear system in Pakistan. Proper strategies should be made to secure the state from cyber-attacks.[565] New technologies along with updated systems should be replaced. Outdated software and systems should be abolished. Cyber awareness and training sessions should be arranged country wide. Experts in information technologies should be hired in every department. The foreign education in cyberspace shall be given to the individuals to learn the new methods of security. Pirated software should be strictly banned. Laws should be there to make the cyberspace deterrent for criminals. The policies shall be updated for better results. Encrypted techniques may be used to secure the information and data on cyberspace.[566]

It is revealed that Pakistan hosted the foreign intelligence agency to make surveillance against its citizens. The US NSA is prominently marked is this regard. Pakistan acted as the third-party partner to provide cooperation for surveillance. Heavy funding is provided by NSA to Pakistani government. Highly advanced technologies are also given to Pakistan which is itself a danger to collect the information and to make surveillance. These technologies are provided in the form of hardware and software with the ability to intercept the information. NSA is working in

[565] John Herhalt, "Cyber crime_ a growing challenge for governments", *KPMG*, (2011).
[566] James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", *Center for Strategic and International Studies*, (2002).

Pakistan at its consulate and embassy. It also maintained its various programs in Pakistan for surveillance like, XKeyscore, Fairview, and Skynet. Through these programs NSA intercepted the phone calls data including audio and written, emails, fax data and internet communication data.

Dialed Number Recognition (DNR) and Dialed Number Identification (DNI) of phone calls records within and outside the country is also intercepted by NSA. About 97 billion of phone calls tapped in 2013 and 11.7 million data from phone calls and internet intercepted in 2012. This interception collected data from mobile phone, internet, computers and emails of Pakistani citizens including their communications with outsiders from country. NSA also installed the record of 55 million people to analyze their phone calls which resulted into the tracking of citizens by NSA agents.[567] It also misidentified a journalist of Al Jazeera as a member of Al Qaida.[568] The revelation of these interception activities protested by the Pakistani government in different episodes in the history. In 2013[569], senators condemned this practice of NSA and in 2014 the Pakistan foreign office officially protested it.[570]

GCHQ is also performing interception and surveillance across the world. It is reported that in 2010 it hacked the Gemalto which is the SIM producing company. In this hacking the GCHQ hacked the phone calls from all over the world. Similarly, it is also reported that GCHQ had stored Kis Key into the Pakistan based networks, Mobilink and Telenor, to collect the voice and text data of cellular communication data from Pakistan.[571] According to another report, it also intervened

[567] Ben Emmerson QC, "the UN Special Rapporteur on counter-terrorism and human rights Two years after Snowden: protecting human rights in an age of mass surveillance Executive summary".
[568] Cora Currier. Glenn Greenwald. and Andrew Fishman. "US government designated prominent Al Jazeera journalist as member of Al Qaeda". The Intercept. 8 May, (2015). (Last accessed: 16 November. 2018)
[569] Ibid;
[570] See for example "Pakistan responds to the NSA Surveillance of PPP". Digital Rights Foundation. 8 July, (2014).
[571] Sadia Rasool. "Cyber security threat in Pakistan: causes Challenges and way forward." *International Scientific Online Journal*, (2015).

into the Pakistan Internet Exchange to make access and hack the information of every user on internet. The spy programs were also installed to make information monitored on regular basis. The reaction of public and political parties was very severe on the revelations of such activities of surveillance. It is the duty of the state to protect the data and information of the citizens. It is also important to protect the cyberspace as it is a security for critical information infrastructures.

Pakistan Internet Exchange is the only system in Pakistan to manage internet and communications on internet within Pakistan. This system is monitored and hacked by foreign agencies. Moreover, PTA also demands interception from service providers. The compliance of this rule let free the service providers to intervene the data of citizens. VPNs and encryption techniques are used to secure the data and the traffic of information.[572] These techniques are banned by PTA in 2011 to monitor Terrorist activities. This impediment resulted into the restriction for citizens to transfer their communications securely and secretly.

5.2 Victimized Sectors of Cyber-Crimes

Cybercrimes are categorized into three types according to the nature of its targets. These crimes have a direct influence on the three levels: Individuals, Organizations and State. According to the targets of cybercrime the magnitudes of these crimes is differ from case to case. As the nature of cybercrime is borderless, it is going to harm all aspects of targets equally. Individuals, organizations and state are common victim for cybercriminals. Even the developed countries are not fully secured from this crime.

[572] J. Haque. "Pakistan's Internet Landscape Report", Bytes for All Pakistan, (2013).

Technology advancement makes it easy to commit the crimes in cyberspace without being revealed before the victims. Developed countries however taken some advanced measures to handle these crimes. Similarly, G8 countries[573] are also equally fighting with these borderless crimes as the nations of third world. But these G8 nations are doing continuous struggle to limit this crime. The creation of World Wide Web (W.W.W) has made it easy to access the information available on cyberspace.[574]

In modern times, the most precious property of an individual is his information existing on internet and cyberspace. Because of advanced nature of transactions, it is unavoidable to control the information about one's bank account, health care, education, tax payments, property records, trade and marketing, i.d card information, marital status, political affiliation and much more. The organizations are also facing the similar insecurity about their sensitive information and data. Moreover, even the states are not secured from this danger. The critical infrastructure is under a threat of invasion from criminals. The various aspects of targets of cyber-crimes may be demarcated into following types according to the nature of its prey.[575]

---

[573] G8 nations are "Britain, Canada, France, Germany, Italy, Japan, Russia and the US".

[574] Michael R Galbreth and Mikhael Shor. "The Impact of Malicious Agents on the Enterprise Software Industry", *MIS Quarterly* 3 (2010), 595-612.

[575] Zibber Mohiuddin. "Cyber Laws in Pakistan: A Situational analysis and Way Forward". Ceericsson Pakistan (PVT.) LTD. 24 June, (2006).

Against Individual Property	Against Organization	Against Society at large
i. Computer vandalism ii. Transmitting virus iii. Unauthorized control/access over computer system iv. Intellectual Property crimes v. Internet time thefts	i. Unauthorized control/access over computer system ii. Possession of unauthorized information iii. Cyber terrorism against the government organization iv. Distribution of pirated software etc.	i. Pornography (basically child pornography) ii. Polluting the youth through indecent exposure iii. Trafficking iv. Financial crimes v. Sale of illegal articles vi. Online gambling vii. Forgery

In traditional crimes, it is difficult to deprive someone from his valuable assets. But in cyberspace it has become more frequent to commit frauds related to money. Cyberspace is technical and complex to understand. Most of the individuals are ignorant from the results of a single click on online world. The digital era is the shelter for dark minds to commit the fraudulent activities and to make the innocent people's prey of their crimes. These crimes are conducted in various ways.

The ultimate result of these crimes is the deprivation of people from their earnings. Those persons are usually the con artists who pay their dirty games very expertly. Unlike the traditional crimes, cyber frauds are committed on internet. People become an easy prey for cyber criminals

because of unawareness from electronic transactions and in this way not only lose their privacy, data, and information but also sometimes damage their social and family life. Along with these damages there is also online harassment in several forms to an individual or a group of people, breaking all barriers of privacy. With the privacy issue at core stage, malware, spamming, web tracking and hacking are important areas of discussion where insecurity from the technological front arises. Therefore, the control and tracking of these crimes are also difficult. The information of an individual is collected and used for committing offence against him. Some types of such financial scams are discussed here. These crimes are mentioned here as they are committed in violation of one's right to privacy of information.[576]

5.2.1 Banking Sectors

Banks are targeted by cyber criminals for financial benefits. This type of fraud is also very common. In this fraud the hackers steal the sensitive and necessary information of the victim to hack the account. The bank account is hacked and money is stolen from the account. Another bank related fraud is the ATM and Credit Cards information stealing. In this situation the device is attached to the ATM machines and the necessary information is read from the card. Later on, this information is used by offender to withdraw the amount by placing this information in his own designed ATM cards through a chip. The banking institutions have shifted to digital technologies in all respects. Financial transactions, records, transfer of money and other marketing are carried on computers. The ATM and credit or debit cards are used as plastic money to transfer or withdraw the funds on computer networks. The whole circle of financial institutions is available on

[576] M D. Goodman, "Why the police don't care about computer crime", *Harvard Journal of Law and Technology* 10, (1997): 465–494.

cyberspace. It is a rich prey for hackers to attack the banks in any aspect. The ATM machines are usually used to read the information on cards. In another instance the online banking system is hacked in recent time in bank Islami and 2.6 million rupees have been stolen. Many other examples of such type of frauds usually occur daily. It is revealed by the Chief of FIA that almost all banks accounts have been compromised. In another example the website of Allied Bank Limited was hacked by hackers along with a message left on it that the security measures are very poor of this bank. This is the matter of threat for economy security of Pakistan. There must be steps to protect the cyberspace to save the money of state and public.

Similarly, Salami attack is a cybercrime related to the financial loss. In this crime software is entered into the system of any organization. Usually, banks or other financial institutions are more prone to become the victim of this crime. The nature of this crime is different to other financial crimes. As this crime is committed by entering a software into the institutions' servers which will collect small amount of money from whole accounts. It is so small amount that it is usually unnoticeable in single attack. In such way the offender may collect a certain amount of money on every occasion without being noticed. Generally, bank employees are involved in this type of crime. The financial institutions are needed to make protections against such type of crimes.

In recent time a bank fraud occurred in a Malaysia based bank in which hackers hacked money by using the fraudulent wires transfers. This is the latest incident in a series of electronic heists at financial institutions around the world. However, no financial lost occurred as reported by bank Negara Malaysia. This was the network of SWIFT Bank Messaging which forwarded the fraudulent wire transfers for money lost. This was the second attack after 2016 attack in which the

amount of $81 million was hacked from Bangladesh Bank. This attack made the financial institutions vigilant to enhance the cyber security on priority basis.[577]

It is reported by the Director of FIA, retired Cap. Mohammad Shoaib that almost all data from Pakistani banks is hacked.[578] He said to the Geo News that maximum banks in the country are compromised. He stated that the banks are the custodian of the money of persons and they should adopt necessary measures to secure the information of people. It was also added by him that the people disclose the theft and banks hide the frauds. No person makes complain to us which is the ultimate reason of loss of money. It is also suggested by him that the banks should take proactive role to control this crime. Shoaib called the meeting of the managing heads from all banks after the alarming situation of security and fraud in BankIslami of Rs. 2.6 million while the international resources told that the amount of robbery was $6 million. He told that about 8000 account of Pakistani banks are hacked and about 100 cases are under investigation in FIA wing.[579] He further reveled that almost six banks have stopped transaction on the basis of debit cards and international transactions on their ATM cards outside the country. In another place, it was also reported that the data of almost 8000 account holders from 10 Pakistani banks has been sold out. A retired Chief Scientist of Khan Research Laboratories reported that his account was lost by Rs. 3 million. He also approached to the Supreme Court for help.[580] This is the matter of immense urgency. To secure the information and data in bank accounts there must be solid legislations. It is also necessary to enhance the confidence of people on their financial institutions. Such type of

---

[577] "Reporting by A. Ananthalakshmi in Kuala Lumpur and Tom Bergin in London"; "Editing by Raju Gopalakrishnan and Nick Zieminski, "Malaysian central bank says foiled attempted cyberheist". 29 March, (2018).

[578] Shahid Iqbal, "Around 10 banks block international payments on debit and credit cards", published in Dawn, 4th November,(2018).

[579] Shakeel Qarar, "Around 10 banks block international payments on debit and credit cards", 06 November, (2018).

[580] Salman Siddiqui. "Banks being hit by cyber attacks: FIA". The Express Tribune. 7 November, (2018).

privacy intrusions is also a danger for state as well. This issue must be addressed and remedied on priority basis to safe the transactions worldwide.[581]

5.2.2 Email and SMS

Electronic mail (email or e-mail) is a method of exchanging messages between people using electronic devices. Historically, the term "electronic mail" was used generically for any electronic document transmission. For example, several writers in the early 1970s used the term to refer to fax document transmission.[582] Email fraud is the intentional deception made for personal gain or to damage another individual through email. Almost as soon as email became widely used, it began to be used as a means to cheat people. Email fraud can take the form of a con or scam. Confidence tricks are required to exploit the inherent greed and dishonesty of their victims. The prospect of a bargain or "something for nothing" can be very tempting. Email fraud, as with other frauds usually targets innocent individuals who put their confidence in get-rich-quick schemes such as investments or offers to sell popular items at very low prices. Many people have lost their life savings due to fraud. [583]

Some common email frauds are mentioned below:

Email bombing is an attack to the victim's email account. In this attack a large number of emails are forwarded to the targeted email account which results into the crackdown of the said account and the destruction of information and data provided on the account of the victim.[584]

---

[581] Kashif ur Rehman and Muhammad Ashfaq, "Examining Online Purchasing Behavior: A Case of Pakistan", International Conference on Social Science and Humanity (IACIT Press): 5.

[582] Luckett, Herbert P. *What's News: Electronic-mail delivery gets started. Popular Science.* Vol. 202 no. 3. Harlan, Iowa: Bonnier Corporation. (1973): 85.

[583] David Wall, *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge: Polity, (2007).

[584] Stefan C. Dombrowski, Karen L. Gischlar and Theo Durst, "Safeguarding Young People from Cyber Pornography and Cyber Sexual Predation: A Major Dilemma of the Internet," *Child Abusive Review* 16 (2007): 153-170.

Moreover, the victim cannot access to his email account and in this way the usual course of transactions is disturbed.[585] It is unlike to the DDoS attacks. In DDoS attack the customers cannot access to the website of a business or cooperation or any other institution. While the email bombing is specifically related to the destruction of email account.

Email spoofing is the attack by using a spoofed email account or website. In this type of cyber attack, the sender shows the wrong information about the email or website.[586] The receiver cannot recognize the spoofed email as a wrong email and he opened it by understanding that it is forwarded from the very source which it is bearing on its face.[587] By opening this spoofed email, the victim shared the required information to the hacker. Usually, such emails come in the name of some companies or institutions. In this way the offender succeeded to gain the desired information.[588] Similarly, spoofed SMS may also be forwarded on mobile phones by using Spoof numbers instead of emails or websites. Spoofed websites may be used to forward spoofing emails.[589] In recent events Pakistan received the spoofed emails from spear phishing documents.[590] In this attack the information of military bodies, government institutions, education departments and health sectors, telecommunication companies and other organization were targeted. The report further revealed that this information was used by criminals to target the sensitive infrastructure of government and military institutions.

---

[585] Majid Yar, *Cyber Crime and Society,* Sage Books, (2006): 51.
[586] Prashant Mali, *A Text Book of Cyber crime and Penalties* (Indiana: Repressed Publishing LLC, 2006), p3.
[587] *Encyclopedia of Cybercrime.* s.v. "fraudulent schemes and theft online", 75.
[588] John Naughton, *A Brief History of the Future The origins of the Internet,* Orion Books Ltd, London, (2001).
[589] Ibid;
[590] Lininger, Rachael and Russell Dean Vines, *Phishing: Cutting the Identity Theft Line*, Indianapolis, IN: Wiley Pub., (2005).

Email is also used as a weapon for cyber stalking. Stalking on internet communication is known as cyber stalking. Cyber stalking is a great threat to privacy in cyberspace. A stalking material is usually forwarded by email, SMS, twitter, Facebook, WhatsApp or any other electronic source. In this situation an individual is stalked on digital world.[591] Any virtual mode is adopted to harass the other person.[592] Usually females are targeted to this crime. It is the harassment by using information technologies and devices.[593] States shall make laws to protect the cyberspace from such type of crime. The victim is generally the weak person as compared to the offender.[594] The organizations and business entities may also be stalked by other organizations to infringe the interests of the weaker.[595]

Advance free Scam is the most common type of fraud which is committed on cyberspace. This scam requires a great level of confidence from the offender as it is directly related to the communications between offender and victim. This fraud is committed for the sake of benefit usually in monetary form. In this popular type of scam, the offender usually forwards an email to the victim for transferring of money in anticipation of receiving something of great value. Usually, the offender offers a heavy amount of money, lottery, gift or some other investment. The ignorant victim is asked to share some necessary information like name, bank account, address, profession and phone number for the fulfilment of necessary requisites. Once the victim shares all such information the fraud may also be committed by hacking his bank account or simply by demanding

---

[591] Black's Law Dictionary, Ist edition.
[592] Petter Gottschalk. *Policing Cyber Crime* (Hershey: Petter Gottschalk & Ventus Publishing ApS, 2010): 35.
[593] Bocij, Paul and Leroy McFarlane, "Online harassment: Towards a definition of cyberstalking", *Prison Service Journal* 139 (2002): 31 - 38.
[594] Michael R Galbreth and Mikhael Shor, "The Impact of Malicious Agents on the Enterprise Software Industry", *MIS Quarterly* 3 (2010): 595-612.
[595] Ibid;

certain money as needed to obtain the large sum of money. The offender usually forwards the email by addressing the victim with his complete name. The email contains the catching story like hey! You have won the lottery of such handsome amount. Or sometimes it may be in the words that you are selected for the prize from this institution and you may collect your amount by fulfilling some requirements. The amount is demanded as procedural fee. These scams mostly attract the greedy peoples who are interested to grab the things of others.

In Pakistan the common examples of this scam are the SMS in the name of cheesy Asma who is always in trouble and demands some balance. The other type of this scam is the Benazir Income Support Program in which the receiver has won the rupees 25000. Similarly, in another Scam of like this a citizen of Pakistan Shehryar Rizwan shares his experience of this fraud. In this case the said person receives an email from the offender who introduces him as a Banker namely, Abdul Rehman from Cimb Bank. He emailed that a deceased person's account having $5.3 million is going to be transferred on the said citizen's name. That citizen was requested to cooperate with the Banker so that the amount may be equally distributed among them. For this purpose, the innocent citizen was asked to transfer the necessary information including name, bank account details, address and profession as well as some amount as procedural fee. PTA has taken initiative in this regard and spread awareness messages for not answering any malicious messages and emails. It also prohibited the citizens for not sharing any information to such malicious email senders. Naseem Masood, FIA prosecutor also reported that people share their data without any authentic verifications of its need.

5.2.3 Software Piracy

Software piracy[596] is a great threat to the security of cyberspace. It is known as the illegal software. It is used without the permission of the owner.[597] Such type of software is a danger to the computers and the information therein.[598] This illegal software is installed into computers without license and copy rights. Later on, such pirated software destroys the whole system or data. Moreover, such software is not the proper protection against hacking of information.

Mr. Muhammad Rehan Farooqi then the Chief Operating Officer of Sysnet told that the original software is helpful to protect the systems and information. It is also legal and benefit for information technology by making cyberspace secure and resistant to attacks. Then the Chairman, Pakistan Council of Information Technology Professionals, Syed Asim Zafar said that genuine software should be made by countries themselves to make their internet privacy stronger.[599] It was also added by him that the legal software will help to control the brain drain in the country by providing them good opportunities in i.t technologies. The BSA spokesman said that the legal software also helps to generate the revenue for country. It was also told that new computers along with original software are assured to be sold in countrywide markets. Raids were made by police to confiscate the pirated software CDs.[600]

Ransomware is the malicious software which is used by criminals to block the access to a system. The targeted system cannot be accessed by the victim and all information is blocked. Sometimes, in the case of encrypted information, the demand is made from the victim to decrypt

---

[596] Digital piracy is also known as copyright infringement and intellectual property crimes.
[597] Majid Yar, *Cyber Crime and Society,* Sage Books, (2006): 51.
[598] Morris, Robert G., Matthew C. Johnson, and George E. Higgins. "The Role of Gender in Predicting the Willingness to Engage in Digital Piracy among College Students", *Criminal Justice Studies* 22, no. 4 (2009): 393-404.
[599] Five held in crackdown on software piracy, Web Desk by Pakistan Press Foundation, 1st January, (2000).
[600] Ibid;

the data. This is the tool to make ransoms from the victims. This software is the hazard for business corporations and persons as it restricts to publish them their necessary information. Sometimes their websites are blocked and the information is controlled unless the ransom is paid. There must be safety measures to protect the systems and information not to be encroached by evil minds. International cooperation should be designed to address this issue at global level. [601]

There are many kinds of trojans. The trojans are used to gain information and data from others' computers. These trojans ate the programs which are used to access, destroy, alter, upload, or steal any information without the permission of the owners. The different types of trojans are used to accomplish different tasks. Remote Administration Trojans (RATs), Password Trojans; Privileges-Elevating Trojan, and Destructive Trojans are the types of trojans. In spite of changing or uploading information, the computer systems can also be destroyed with the help of these trojans. Moreover, viruses are also transferred with the help of these trojans. There must be measures to detect such trojans on online networks or in the form of programs. This is the easy source of destroying the information and data on a large scale.

Key logger is the observation of one's key strokes to collect the information.[602] There are various ways to monitor the key board activities to gather the typed information. It may be in the form of hardware device which is directly attached to the computer to collect the information. It may also be in software program which collects the information of the user. Keyloggers are the spying program to monitor the computer activity of the targeted person. It can damage the gross

[601] Peter Grabosky, "The Global Dimension of Cybercrime", *Global Crime* 6.1 (2004): 146 - 157.

[602] "Keystroke logger is a software that captures what is typed and sends it to a remote location. It is useful for stealing passwords, credit card numbers, and other confidential information".

level of networks if installed into banks or other business sectors as it monitors and collects every stroke of the victim's keyboard.

Malicious Mobile Code is a recent term to describe all types of malware, trojans, viruses, worms and rouge internet codes. It is spread to damage the computers and networks. It travels from computer to computer and network to network. It destroys and alters the information without the consent of the operator or owner. In this era of technology, the information and data are on risk. The persons rely on the networks and computers to keep their records.[603] But the bad people are trying to damage their work with the creation of malware. It is required that expert professionals should be consulted to protect the data. Updated anti-viruses should be installed. The original software shall be purchased.

5.2.4 Social Media

social media is frequently used to commit cyber-crimes. The usual type of social media crime is the creation of fake email and other social media accounts in the name of some other person instead of the real account holder's name. Mostly the famous personalities names are used for this purpose. In this crime the fake accounts are made on internet. In this unsecured cyberspace it is very common and easy job to make the fake accounts. Almost all type of social media may be used for this purpose. In Pakistan this practice is also very common. A report of Cable News Network revealed that about 83 million Facebook accounts are fake.[604] The teen age girls are targeted to create such type of fake accounts in their names. However, some fake business entities also make fake accounts in the name of famous companies to loss their reputation.

---

[603] Richard S. Murphy. "Property Rights in Personal Information: An Economic Defense of Privacy", 84 *GEO. L.J.* 2397, (1996).

[604] Aaushi Shah and Ravi Srinidhi, *A to Z ofcyber-crime* (Pune: Asian School of Cyber Laws, 2012), 150.

5.2.5: Websites

Websites are a great source of online frauds. Creation of fake websites is a very frequent cyber-crime on internet through. The fake websites are created to defeat the public.[605] It is usually happened in the name of educational institutions or business companies. The common people are made the target of this fraud by presenting the fake websites as the real one.[606] To create the anonymity, the nature, name and ideas are kept similar to the real websites. The pictures of events from the original websites and other information are also updated by fake websites.[607] The sensitive information is seeking in the name of real website. Likewise, the financial loss may be happened if it is the website of some business company like amazon Draz or ebay etc.

Distributed Denial of Service Attack (DDoS) or Denial of Service Attack (DoS) is a type of cyber-attack.[608] In this attack a website is blocked by sending a large volume of gigabits per second (Gbps).[609] It is reported that in 2013 the 20 Gbps were forwarded to control the Pakistani websites while in 2014, the events raised to 100 times more severe. In 2014 the 100 Gbps were reported to block the various websites in Pakistan. Even many important websites were defaced by hackers. The websites of security forces and federal government were approached by hackers. Many important information was stolen from these websites. The data of security forces and government institutions was taken from these attacks.

FIA claimed that the Pakistani websites are not secure to resist such attacks. It asserted that Pakistani ISPs are not so secure to manage the DDoS of even 5 Gbps. Further, an official of FIA

---

[605] Michael R Galbreth and Mikhael Shor. "The Impact of Malicious Agents on the Enterprise Software Industry", *MIS Quarterly* 3 (2010): 595-612.
[606] Ibid;
[607] Aaushi Shah and Ravi Srinidhi, *A to Z ofcyber-crime*, Pune: Asian School of Cyber Laws, (2012): 150.
[608] Majid Yar, *Cyber Crime and Society,* Sage Books, (2006): 51.
[609] Prashant Mali, *A Text Book of Cyber crime and Penalties*, Cyber law, 46.

said that a strong and competent force is needed to tackle these issues. A report revealed that India attacked Pakistani websites on Pakistan's Independence Day, August 14. In reply the Pakistani hackers also attacked the Indian websites on 15th August.[610] Such type of attacks is very dangerous for websites of sensitive institutions and business entities. As these attacks block the access to hacked websites and take the control over such websites. It results into severe financial loss along with the loss of information and data.

Web Defacement in another type of cyber-crime. In this crime the targeted website is defaced by placing false information on the victimized website. Mostly the religious and political websites are defaced to represent the beliefs of their faith. Financial institutions' websites are also hacked and defaced to commit some financial crimes.[611] The organizations fame is destroyed by posting some obscene material. Similarly, the websites are also hacked and defaced to collect the sensitive information about corporations. Customer's data may also be gathered from hacking of financial websites. Public trust is lost by such hacking and it results into loss of business of some particular company. Moreover, the government sensitive information may also be collected by the enemies of the states. A proper legislation and its implementation should be made to protect the information and data. Similarly, there must be some protective measures to make websites immune from intrusions.

Another website related crime is the web jacking. Web jacking is the controlling of websites on the basis of force. Sometimes the criminals with strong skills take the control over the government institutions' website to fulfill their demands. Mostly the financial or political purposes

---

[610] Talha Khan, "Cybercrimes: Pakistan lacks facilities to trace hackers", The Express Tribune, 1st February, (2015).
[611] David Decary-Hetu, and Benoit Dupont, "The Social Network of Hackers", *Global Crime* 13, no. 3 (2012): 160-75.

are fulfilled by committing this crime. This is the breach of institution's privacy to take the control of its website. The website of Supreme Court was hijacked to make some political demands fulfilled.[612] The website of Supreme Court is hacked occasionally by hackers in the past history. Similarly, the other government institutions, websites are hacked by hackers[613] to make some ransoms.[614]

5.2.6 Internet

The proliferation of technology is a giant. It is a great danger to the information available on internet, computers, devices, software, mobile phones and other systems. This has been created a threat for the security of the persons and the states. The people and nation both are in danger for the invasion into their privacy. The availability of internet and the nature of technology has made it impossible to control the flow of information and data. As it has been discussed earlier in the beginning of this chapter that in Pakistan there are many cybercrimes which are a regular hazard for the security of information in cyberspace. The whole system of the business has been shifted on technologies.

The critical infrastructures, grid stations, business companies, banking industries, government databases and the education sectors have been shifted on internet. Cyberspace is also as important for the security of a state as the other territories. Cyber warfare is the future threat for the security of a country. It has been said by the Roger's Molander, an expert on the RAND corporation, that the national security is dependent on the cyber security. Robert Dahl says that the power is the

---

[612] Two hackers were involved in hacking the Supreme Court website, one was Pakistani national and other was Indian national.
[613] Robert Schifreen, *Defeating the Hacker: A non-technical guide to computer security,* Wiley, (2006).
[614] Ibid;

ability to force people to make them to do what you want to be done. Now a days, cyberspace is playing a role to capture the brains of people by setting the desired trends. People are traced by tracking their information on cyberspace. Cyberspace is like a power culture to capture the behaviour of the other persons. Social networking sites are used for this purpose. Pakistan is the rapid growing market for the internet industries in the South Asia region. Pakistan is one of those countries which introduced internet services mainly in urban area. According to the report of PTA, 120 million of Pakistan population has become dependent on cellular phones. Similarly, internet users are also present in the Pakistan. The ratio of internet use is growing day by day. Internet is used by evil minds to commit cyber-crimes. Following are the examples of frauds which are carried on internet;

Data Diddling on internet is a kind of fraud, the virtual data is altered. The real information is changed. It is the type of the dangerous infringement of privacy in cyberspace. As the information and data is changed from the original one.[615] The data may be related to health, education, bank accounts or tax payments. The organizations may be the victim of this fraud. The business companies may face a great injury in case of data diddling of its customers or shareholders. Institutions may become a prey of this curse as it is very difficult to be highlighted within short time. Financial loss may also be made by altering the data of organizations. Strict measures should be taken to protect the information and data from diddling.[616]

---

[615] Marjie T. Britz," A New Paradigm of Organized Crime in the United States: Criminal Syndicates, Cyber-gangs, and the Worldwide Web", *Sociology Compass* 2, no. 6 (2008).

[616] Dr. Taimur, Rahman, "The Internet, Youth and Education in Pakistan", National Human Development Report 2015, November, (2015).

Identity fraud is a type of fraud which is committed on internet to hide the recognition of someone.[617] In this crime the offender uses the name of other person to make communications with other people. This type of crime is usually committed to deceive someone or to steal some important information. Generally, the financial frauds are committed in this way by acquiring the information about accounts and credit cards.[618]

Internet time theft is a crime in which one person uses the internet hours paid by another person by gaining illegal access to his ISP or Id and passwords. By acquiring such access, the wrong doer also gain entry to the information and data of the owners from his computer. In this way the unauthorized person may change any information or may copy this information.[619] He can also destroy the system or information. He may also transfer some spyware or malware to the system for future access or damage of information. Such information may be transferred to some other source. This theft may cause financial damage as well.[620]

Similarly, stock Robot Manipulation crime is committed to manipulate the stock marketing. In this crime a program is used to influence the stock marketing. The fake sale and purchase are made in this program. Later on, the actual sale and purchase is made automatically by making reasonable profit margins. This type of program is not allowed in marketing. It is against

---

[617] Ahsan Latif Imam, "Cyber Crime in Pakistan: Serious Threat but No Laws!" http://blogs.tribune.com.pk/story/15063/cyber-crime-in-pakistan-serious-threat-but-no-laws/ (Last accessed: 16 November, 2018).

[618] Dr. Taimur, Rahman, "The Internet, Youth and Education in Pakistan", National Human Development Report 2015, November, (2015).

[619] Jerry Kang, "Information Privacy in Cyberspace Transactions". 50 *Stan. L. Rev.* 1241 (1998).

[620] Marjie T. Britz," A New Paradigm of Organized Crime in the United States: Criminal Syndicates, Cyber-gangs, and the Worldwide Web", *Sociology Compass* 2, no. 6 (2008).

the principles of morality and trade. The person may suffer great financial loss in this way. The states should strictly monitor the business industries for such type of mal practices.[621]

Like conventional defamation, the cyber defamation is also a crime. Cyber defamation is committed to defame a person, organization or institution by using the computer or internet. The essential requirements to commit the cyber defamation are the false statements that must be going to the victim or his family and this defamatory statement is published by electronic sources. The statement must be made with the intention to defame the targeted subject.[622] It is the matter of great concern as it is related to the repute of a person or some institution. Technology has made it convenient to spread any information within the spur of the moment. If a defamatory statement is published to defame some business company or corporation. It will harm its reputation within the short span of time. These immoral strategies are usually adopted by competitors to defame the name of any business rivals.[623] The privacy is compromised in this way. The victims bear irreparable loss by such activities. As it has already been discussed that the reputation and honor of a person is inviolable. States shall make such laws to protect the repute and fame of a person in digital world as well. Technology advancement also requires the advanced measures of protection and security to make the people safe in cyberspace.

Virus Attacks are the programs which may be transferred through downloading of certain infected files from internet. It may also come from attachments of emails or from funny images. Sometimes, it is transferred from audio or video files. This program destroys the information and

[621] Ibid;
[622] Zibber Mohiuddin. "A paper presented on: Cyber Laws in Pakistan: A situational Analysis and way forward". (International Judicial Conference on June 24, 2006 Supreme Court of Pakistan Islamabad): 17.
[623] Ibid;

data from the victim's computer. These are also forwarded to make installation of fake passwords in order to open a certain file and in this way gets entry to steal some information from system.[624] The virus further spread to other systems from the email account of the victim. The whole data is corrupted and deleted by this virus. It may be spread deliberately by offenders to destroy the information and data of the targeted victim. The victim may be the individual or an organization or even the state.

Similarly, worm attack is a standalone malware computer program. It has the ability to replicate itself to spread on the computer systems. It is usually entered into a computer because of some failure into the security measures of a computer. Worm attack is mostly entered into a computer through internet and computer networks. Unlike the virus attack it does not need any computer file to spread itself. It damages the space on computer`s memory. This malware is a great danger to the information and data available on computers. Hackers forward this worm to destroy the information and computers of the targeted persons or organizations. It is also the threat for state`s security. It is used to harm the critical infrastructure of a state. "I LOVE YOU" worm is the example of this malware which was spread to destroy the computers of different states. Iranian nuclear system was also attacked by this virus.[625]

With the development of information age and internet, the terrorist organizations have also adopted the cyberspace to conduct terrorist activities.[626] Any disruptive activity with the intention

---

[624] Jeremy Clarke and Urs Hengartner, "Panic Passwords: Authenticating under Duress", *School of Computer Science : University of Waterloo*, (2008).

[625] Niall Firth. "Computer Super-virus 'targeted Iranian Nuclear Power Station' but Who Made It?" http. www.dailymail.co.uk sciencetech article-1314580/Stuxnet-worm-targeted-Iranian-nuclear-power-station-sophisticated-virus-attack-ever.html. (Last accessed: 16 Nov, 2018).

[626] Ibid;

to destruct the religious, political or social believes of some person or community in cyberspace amounts cyber terrorism.[627]

Encryption communication is carried on in codified form so that the real massage cannot be understood. Such type of communication is conducted to secure the data from stealing. The terrorists commonly use this method of communication to secure their messages from intrusions.[628] Moreover, the information on computer systems is also secured in encrypted form which make it impossible for law enforcement institutions to read this data. There must such techniques which may make it possible to read the encrypted communication of terrorists.[629] States are responsible to curb the terrorist activities on its territory. Similarly, the cyberspace should be free from such activities. There should be no danger to the public of being victimization from terrorist activities. In case of the security of a state such activities are a great threat to its security. [630] The state should draft such laws to control these practices from the root level. Sometimes the critical infrastructures are hacked by terrorists to achieve their motives.

5.3 Critical Analysis of Cyber Legislation of Pakistan

Pakistan is not updated in cyber laws. The first endeavor in this regard by the Government of Pakistan was the passing of "Electronic Transaction Ordinance (ETO), 2002". ETO introduced the concept of E-Commerce in the country.[631] ETO provided the laws for the regulation of information and data in cyberspace. It makes the provisions for the regulation of electronic communications.

---

[627] The above definition was proposed by Rohas Nagpal, President, "Asian School of Cyber Laws in the paper titled *Cyber Terrorism in the context of Globalization* presented at World Congress for Informatics and Law II held in Madrid", Spain in 2002.
[628] Ibid;
[629] "The USA PATRIOT Act which was passed on 26th October, (2001)".
[630] David Wall, *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge: Polity, (2007).
[631] Adnan Chaudhry. "Content Regulation in Pakistan's Digital Spaces June 2018". HRC Report, (2017).

It provides the measures for the safety of electronic records, information, banking and other business transactions. ETO ordinance declared many criminal activities as cybercrimes. This was the first legislation of the country to control the electronic communications in the country. However, this ordinance has also many grey areas. It overlooked many crimes which were mentioned in various international cyber laws of different countries.[632]

It is also the outdated legislation as no update is made in it to meet the speed of new technologies and the new cybercrimes.[633] ETO remained the sole legislation to deal with the cybercrimes till the passing of PECA, 2016. In these fourteen years, from 2002 to 2016, ETO was the only law to combat with highly advanced technology generated crimes. Because of insufficient capacity to deal with new cybercrimes many crimes and criminals went unaddressed. This was the era when cybercrimes raised at their peak in Pakistan. People were exploited due to the absence of any legal remedies. Pakistan, being a developing economy, should make proper cyber laws to provide the safety in cyberspace.

As the business communications and banking transactions may be protected by making adequate laws. It may also be considered that every sector of business and government have their own regulations and enforcement mechanism so that the information and data may be more secured in cyberspace. Similarly, institutions should have their own cyber laws to conduct their communications in safe hands.

However, in 2007 and 2009 two Ordinances "Prevention of Electronic Crimes Ordinance (PECO), 2007 and 2009" were adopted to tackle with cybercrimes. But these ordinances (PECO,

---

[632] KPMG, *Global eFraud Survey*, KPMG Forensic and Litigation Services, (2013).
[633] Ghulam Muhammad Kundi, *E-Business in Pakistan: Opportunities and Threats*, Lap-Lambert Academic Publishing, Germany, (2010).

2007 and 2009) could not sustain due to the failure of seeking permission from Parliament. In 2007, PECO was introduced in the cyber legal framework of Pakistan. This ordinance was named as the Prevention of Electronic Crimes Ordinance (PECO), 2007.[634] The major purpose of PECO was to fight with various unaddressed cybercrimes. Cyber stalking and cyber spamming were introduced as cyber-crimes in this ordinance. These crimes were properly defined in this legislation. Moreover, the proper regulation was provided for internet sectors by this ordinance. Further this ordinance also announced the punishments for different type of cybercrimes. Seventeen types of offences were highlighted in this ordinance with a different range of punishments starting from six months to the death penalty according to the nature and effects of crimes. Cyber terrorism was also mentioned in this ordinance.

This ordinance (PECO) was quite updated and modified according to the advancement of cybercrimes. This legislation was tried to cope the need of the time for proper laws in cyberspace. This ordinance also authorized the service providers to retain the traffic data for 90 days. Other necessary standards were also mentioned for internet service providers to make the minimum approach towards cybercrimes but this ordinance was not sufficient as it did not speak about the enforcement policy. Further, it did not clearly talk about the situations for the retention of data by service providers. Which was the compromise with right to privacy of individuals. Moreover, the authority can intervene with data and information without the warrant of court. Therefore, this ordinance was also the interference with the privacy of information and security of data. This ordinance became ineffective in 2009. With the lapse of this ordinance, the legal regime of the country once again become dependent on ETO,2002 which was insufficient for modern

[634] https://ipop.org.pk/wp-content/uploads/2019/08/PECO-2007.PDF

cybercrimes.[635] This made the law enforcement agencies paralyzed to punish offenders and to remedied victims.

In the aftermath of Peshawar attack, a cybercrime bill was introduced in response to the National action Plan to curb the terrorism activities in Pakistan.[636] This bill was finally become Act in 2016 and named as "The Prevention of Electronic Crimes Act, (PECA) 2016".[637] The main purpose of this Act was to control the cybercrimes and to penalize the cyber criminals with heavy punishments. However, this Act allowed the unfettered liberty to the authorities to monitor the militants. Under this Act many liberties of the individuals are compromised. This Act is the limitation on various rights of the people. Surveillance, monitoring, censorship and the restrictions on freedom of speech and expression are allowed in this Act.[638]

This Act is the restraint to the right to privacy as the investigating authorities have the large number of powers to search, seize and monitor the data and information. The investigating agency, FIA, is empowered with a power to arrest some person without the warrant. Similarly, the warrant is also not necessary for monitoring, copying, seizing or removing any contents of data. The provisions regarding warrant are just permissive not compulsory. The word "May" is used to take the warrant of a court. These unfettered and unbridled powers of investigation agency will lead to the misuse of the powers as witnessed in the history of PECO, 2007 and 2009. It is also noticeable that even the arrest may also be made by the agent of investigation agency without the warrant of the court.

---

[635] Munir, Muhammad Amir. "Electronic crimes ordinance: an overview of its preamble and extent." *Pakistan Journal of Criminology* 2, no. 1 (2010): 189-202.
[636] Jamal Shahid, 'Flawed' Cybercrime Bill Approved. Dawn News. 17 April, (2015).
[637] Prevention of Electronic Crimes Act, 2016 (Act No.XL of 2016).
[638] Ibid;

Sections 30-32, 34 and 36 allow investigating agency to proceed even without warrant of court. It allows the chances of political abuse as no necessity is described for the controlling, monitoring or seizing of data. Moreover, the contents of section 34 are also too vague to define that which type of data amounts to be a threat for the national security, glory of Islam or the friendly relations of Pakistan. Sections 14-17, 22, 23, 27-33, and 45 are also vague and not properly defined.

Sections 18 and 21 respectively are also an attack on freedom of journalists.[639] As no clear demarcation is drawn between the right to privacy and freedom of expression in these two sections, Section 18 is related to the criminalization of any false transmission of intelligence information with intent to infringe the repute of the person. Further, section 18 is against the freedom of expression and journalists. While section 21 is related to the cyber stalking which includes the sharing of a person without his consent is liable to criminalization under this section. As it is observed that the provisions are not properly segregated from the right to privacy of a person and freedom of expression. Section 21 is also not clearly elaborated. The right to privacy and freedom of expression is not properly balanced in this section. It is also the matter of explanation for the truly enforcement of rights. In the same way section 34 does not highlight the situation to be against the state's security, glory of Islam or friendly relations with other states.

The definition clause of the PECA, 2016 is vague and blurred. It is observed that the certain definitions like, act, access to information system, unauthorized access, damage to the information system, critical infrastructure, interference with information system or data, dishonest intention are not properly defined. If these definitions are ambiguous then how the certain acts may be

[639] Aleem, Yasir, Muhammad Asif, Mohid Khaliq, Iqra Imtiaz, and Muhammad Umair Ashraf. "The Prevention of Electronic Crimes Act 2016 And Shrinking Space for Online Expression in Pakistan." *Al-Qalam* 25, no. 2. (2020): 1-12.

amounted to crimes. These definitions may be again abused to make some political or other alike benefits. Section 3 to 8 are also appeared as giving room for broad and vague interpretations. Civil liberties are also restricted in these provisions. Dishonest intention is not clearly and specifically defined in these sections. In his speech to the UN General Assembly, David Kaye the UN Special Rapporteur said that if there is a clash between the liberties and restrictions, the liberties should be preferred which should provide the space for freedom of expression in the public interest.[640] State should make the provisions of PECA clearer and more understandable. Sections 9 and 10 are also needed to be elaborated in clear meanings. These sections are very broad and may be implemented in any type of expression. The term "Terrorism" is needed to be discussed in the preview of specific sense. It is also very broader term and implemented in general sense of terror. Manty persons in the history are convicted by making them criminate in the ambit of terrorism.

The examples of Saqlain haider[641] and Rizwan haider[642] are also present. They were sentenced for making hate speech. Similarly, sections 13 and 16 are also against the freedom of expression and privacy of persons. These sections restrict the encryption techniques which is against the privacy of information and data.[643] By adopting the encrypting techniques people may save their information. Government should make such liberties unrestricted and unfettered.

As the freedom of expression is compromised under the blanket of reputation of a person, the clear segregation of public policy and freedom of expression may be identified to preserve the

---

[640] D. Kaye, "Report on Protection of Sources and Whistleblowers". (2015) https://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/361.(Last accessed: 16 Nov, 2018).

[641] Baloch, Haroon. "Internet Rights and Legislation in Pakistan: A Critique on Cyber Crime Bill, 2016." *Accessed on 23rd June* (2016).

[642] Ibid;

[643] Section 13 & 16 of PECA, (2016).

privacy of a person. The illustration of former interior minister Rehman Malik may be recalled who delayed the flight. He was forced by passengers to offload and the video became viral of this incident. If this Act had been promulgated at that time, then the minister could take the benefit of this clause for harming his reputation. However, it was his fault and the matter was of public interest. Such type of issues is needed to be specifically addressed by the state to deal with these rights.

Section 39 is also a debatable section. In this section the federal Government is authorized to make cooperation with foreign governments. In this regard the federal government may transfer any data or information to the foreign investigating agency without the permission of the court. The provisions of this section are a clear violation of the right to privacy of information and data in cyberspace. Moreover, it is the compromise with the right to privacy of a person and such act of federal government is not challengeable in any court. It also legalizes the previous practices of the government of sharing data with NSA and British`s GCHQ. In this type of data every form of information is included whether in the form of audio, video, images, documents and texts. The state should not compromise the privacy of its citizens in such a gross way. There must be some safeguards to shield the personal information of a person. This sharing is also a threat for the security of the state itself. This act is also criticized by United Nations and International Rights Organization (IRO) because of its harsh restrictions.[644] It is also discussed that this is the flaw full legislation as no demarcation is made on right to privacy of a person. The freedom of expression is also compromised, and the cyber terrorism is also not properly defined.[645]

---

[644] Report of Freedom House. "Freedom on the Net 2017." 01 Jan. (2017).

[645] Zahid Jamil, *Cyber Law*, Presented at "the 50th anniversary celebrations of the Supreme Court of Pakistan International Judicial Conference on 11-14 August", (2006).

Insufficient Data Protection Laws in Pakistan:

There is no sound legislation on the protection of data in Pakistan.[646] The right to privacy is protected and guaranteed in the constitution of Pakistan as the fundamental right.[647] However, no effort has been made to protect the information and privacy of a person in cyberspace. Cyberspace is a major dilemma of 21st century. People share their information on the cyberspace for different purposes. Business records, banking transaction and other communications are made on internet by sharing data and information. It is the duty of the state to provide a crime free cyberspace to its citizens so that the security of both i.e., the country's security and the person's security may be protected. It is the responsibility of the state to make adequate laws for the protection of information and data. With the development of technology and the reliance upon these technologies it is the need of the time to make data protection laws to regulate the data in cyberspace. The borderless nature of cyberspace makes it a threat for the privacy of a person to be compromised. In this regard the state should make appropriate data protection laws for the different sectors of the business. Some data regulating authority should also be established to keep the data safe. In the absence of data protection legislation, there are some other laws which are utilized to secure the information and data in cyberspace. Before the enactment of PECA (2016), only the ETO (2002) was there to regulate the data safety and security breaches. Section 36 of the ETO,2002 was invoked to cater the matters of data and information intrusions. The unauthorized and illegal access to data and information was punished under this section. With the enactment of PECA,2016 the section 36 of the ETO,2002 became inoperative and lapsed. Now the provisions

[646] Report of Privacy International, "State of Privacy Pakistan," 01 Jan. (2018).
[647] Part II of Constitution. (1973).

of PECA, 2016 deal with the crimes of privacy invasion into information and data. Unauthorized and criminal access, alteration, transfer, copying of any information or data is punishable under this Act. Similarly, the provision of PECA also protects the privacy of the state.

As Pakistan has no sufficient laws to secure the data and communications. NADRA is at risk to compromise the data of citizens. It is reported that the Shah Faisal Branch of NADRA at Karachi was hacked by some device and the data was stolen. In 2012, a Turkish hacker also talked about having access to the NADRA website by hacking through backdoor. He further revealed about the hacking of FIA website. Similarly, SIM cards are also necessary to be registered. However, this registration is also a silent compromise with the right to privacy as it allows the interception of phone calls and data. Moreover, there is a lack of awareness about the privacy right in digital sphere. The service providers of mobile companies also provide no facility of complaints about privacy breach on their websites.

No individual cannot access to the information of the state which is not made for public access. The Government employees are also restricted to share such information with other states. However, the state and its Investigating agency are at liberty to share the information and data of a person with other countries and their organizations to make the international cooperation. The right to access to information Act, 2017[648] also provides some limitation to the right of information. According to this Act the information cannot be shared if it is creating some danger to the privacy of a person. In this way, the right to information is also compromised in section 17 for the sake of privacy of a person. Women are at more risk for the infringement of right to privacy.[649]

---

[648] Government of Pakistan, "The right to access to information Act", (2017).
[649] Report of Digital Rights Foundation. "Surveillance of Female Journalists in Pakistan". (2016).

Situation of Right to Privacy in Existing Regulatory and Legal Framework:

Right to privacy is facing much constraints in Pakistan. This right is not provided to the individuals without the compromises. The right to privacy is interfered by many policies and formalities in Pakistan.[650] Sometimes this right is not even acknowledged. Although, this right is guaranteed in the constitution. Despite the fact that it is the fundamental right of a person. This right is probably most compromised and neglected right in cyberspace. However, this right is of great value for the security of the person and a state. Internet is over regulated by the authorities and this right is not freely exercised in Pakistan.[651] It is reported by the freedom house in its report on "freedom on net" that the privacy is not free in Pakistan and it is suppressive.[652] Further, it is also stated that even the Pakistan Telecommunication Authority (PTA) has banned the study of the report taken by Freedom House.[653]

The right to privacy is endorsed in "Right to Fair Trial Act, 2013"[654] and "Prevention of Electronic Crimes Act, (PECA) 2016". The right to privacy is adopted in these laws to bring this right in line as provided in the article 14 (1) of the constitution, 1973. However, the right to privacy is exercised with restrictions and intrusions of government and private organizations. This results into the narrow enforcement of privacy and data protection rights. Moreover, there is no data protection law to date. The Electronic Data Privacy Bill, 2005 is still waiting for the assent to become Act. In the absence of adequate legal regime many cases of data privacy remain

---

[650] Ibid;

[651] Privacy International, "State of Privacy Pakistan," 01 Jan. (2018). Online available and retrieved from: https://privacyinternational.org/state-privacy/1008/state-privacy-pakistan (Last accessed: 16 November, 2018).

[652] "Freedom on the Net 2016, Country Profile: Pakistan", Freedom on the Net 2016, Freedom House, 14 Nov. 2016, www.freedomhouse.org/report/freedom-net/2016/pakistan (Last accessed: 16 November, 2018).

[653] PTA blocks Freedom on the Net Report, https://propakistani.pk/2017/11/17/pta-blocks-freedom-net-report-pakistan/ (Last accessed: 16 November, 2018).

[654] Investigation for Fair Trials Act, National Assembly of Pakistan, 22 February, (2013).

unheard.[655] Article 14 (1) of Constitution, 1973 protects the privacy of one's home. However, there is no explicit provision to protect and shield the privacy of communications, information and data in cyberspace. Moreover, there are not any specifications of limitations that restrict the right to privacy in the preview of necessity and public interest. The information and data provided in cyberspace is not secured by clear laws. There are certain grey areas in the existing legal framework which must be updated to secure the information in cyberspace.

Privacy is encroached equally by public and private sectors. Journalists, women, minorities, human rights activists and other common people are identical in the privacy intrusions.[656] Their right to privacy is compromised under the blanket of surveillance by state. This surveillance is carried on by the cooperation and partnership with foreign agencies.[657] The surveillance is carried out by government and law enforcing agencies without the consent of the persons. Such surveillance is done as the part of National Action Plan[658] to monitor the terrorist activities. The knowledge and consent must be made compulsory to such surveillance. So that, the people may be aware of loss of their privacy loss and disclosure of necessary information. This monitoring is the infringement of civil liberties as well.

It is also a threat to share the personal information on public and private companies' websites. No security measures and safeguards are provided by organizations for securing the data of the persons. There must be such laws as to make obligations on data collection institutions to

---

[655] Sadia Rasool. "Cyber security threat in Pakistan: causes Challenges and way forward." *International Scientific Online Journal*, (2015).

[656] Ibid;

[657] "Liberty and security in a changing world: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies", 12 December, (2013), Recommendation 4,25, online at: www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (Last accessed: 16 November, 2018)

[658] "The National Action Plan (NAP) was adopted after the terrorist attack on Army Public School, Peshawar in 2014". This Act was designed to curb the terrorist activities in the country.

keep safe and secure the data of the individuals. It is observed that NADRA[659] is the largest database in the world. However, no security measures are adopted by government to protect this database. In contrast, this database of NADRA is used to track the identification of a person or to make intervention into one's privacy.[660]

Social media websites also provide the opportunities to track the data and information of persons. Facebook also contracted with government of Pakistan to take the control to monitor blasphemy cases. It is the opinion of human rights activists that this agreement is in the infringement of right to privacy and freedom of expression.[661] Lahore High Court also asked government of Punjab to observe the online material for hate speech.[662] Similarly, the government of Punjab has also its own monitoring authority. It has established a Punjab Safe Cities Authority and an observing cell under the power of this authority.[663] Without the clear demarcation of laws relating to the right to privacy and limits on freedom of speech it is not justified to monitor the persons in cyberspace.

Government had also observed the persons with the help of Inter-Service Intelligence Agency and NSA of America.[664] This surveillance was without the knowledge and consent of the

---

[659] Government of Pakistan, "The National Database and Registration Authority Ordinance", (2000).
[660] A.S. Elmaghraby & M.M. Losavio, "Cyber security challenges in Smart Cities: Safety, security and privacy", *Journal of Advanced Research*, vol. 5, no. 4, (2014): 491-497.
[661] Pakistan World Press Freedom Index 2017. "Reporters Without Borders". https://rsf.org/en/pakistan (Last accessed: 16 November, 2018)
[662] Ibid;
[663] Munir, Muhammad Amir. "Draft Pakistan Electronic Crimes Act, 2004: The Proposed E-Law in a Judge's Perspective." *Pakistan Law Journal* (2005): 333.
[664] "Briefing on Privacy International Legal Case: 10 Human Rights Organisations v. the United Kingdom," Privacy International, July 21, (2015), https://www.privacyinternational.org/sites/default/files/2018-02/Privacy-International-Legal-Briefing-10-Human.pdf. (Last accessed: 16 November, 2018).

people of Pakistan.[665] In another instance many cellular companies were monitoring the information and data of Pakistani people without their permission. Such type of secret surveillance is dangerous as sometime important information is transferred in ignorance. "Alcatel, Ericsson, Huawei, SS8 and Utimaco" are the prominent companies which were engaged in plan of making network of mass surveillance.[666] Huawei, a china-based company, is hired to make observation and monitoring availability under the safe city project.[667] The government of Pakistan should take necessary safeguard to monitor through these foreign companies. As the important information is shared with foreign states which is a danger to the national security. There should be necessary protocols and regulations for such monitoring and surveillance plans.

Due to the lack of necessary safeguards Pakistan has also faced the hacking of Pakistan Internet Exchange (PIE) by the British GCHQ.[668] and consequently the data of Pakistani citizen's become targeted. As the data could be accessed and stored by this hacking. In another case, the NADRA database was made accessible to US agency NSA.[669] Similarly, it is also revealed that the USA has also encroached over 55 million phone calls by SKYNET program.[670] Such type of intrusion is the infringement of right to privacy and it must be secured by the states. State should

---

[665] "FAD FY 12 CCP Funding of Partners". National Security Agency slide reproduced in Glenn Greenwald, No Place to Hide, p. 124. http://glenngreenwald.net/pdf/NoPlaceToHide-Documents-Compressed.pdf (Last accessed: 16 November, 2018).

[666] "Liberty and security in a changing world: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies", 12 December, (2013), Recommendation 4, p25, online at: www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (Last accessed: 16 November, 2018).

[667] M. Rice, "Tipping the scales: Security & surveillance in Pakistan". (2015). https://www.privacyinternational.org/sites/default/files/Pakistan%20report%20high%20res%20201506?2_0.pdf (Last accessed: 16 November, 2018).

[668] J Lanchester, "The Snowden files: Why the British public should be worried about GCHQ", The Guardian 3 October, (2014).

[669] "Report of the Senate Committee on Defence and Defence Production, Senate of Pakistan, August-September", (2013), http://www.senate.gov.pk/uploads/documents/1378101137_113.pdf (Last accessed: 16 November, 2018

[670] Barton Gellman and Ashkan Soltani, "NSA tracking cellphone locations worldwide: Snowden documents show", Washington Post, 4 December, (2013).

make such measures as to monitor the data of its nationals by itself. It will be beneficial for the security of state itself.

Surveillance and monitoring of information can be done only for legitimate purposes.[671] These legitimate purposes may be the safety of the national security, freedom of information, prevention of hate speech, the control of terrorism and likewise. Unjustified and unauthorized intervention into information is the infringement of the right to privacy. The service provider may retain the data under the provisions of PECA for the period of one year or the period as specified by the authority. This period is not justified according to the Office of the High Commission for Human Right (OHCR). It is further stated that this period is against the provisions of ICCPR.[672] Justified and reasonable grounds should be provided for the retention of data. Such period will make the service providers more controlling and influential to interfere with the privacy of individuals. State should make clear provisions for such type of orders. There shall be no ambiguity in these provisions so that there must be a balance between the privacy and exercise of power to retain traffic data.

The Monitoring and Reconciliation of Telephony Traffic Regulations 2010 (MRTTR), demands from the service providers to monitor and intervene the data provided on networks. This interference and surveillance are the condition for giving the license to operate the network company. If the network provider does not make contract to access and monitor the data, the PTA does not award him the license and permission to carry on networking operation services.[673]

---

[671] The UNGA Resolution 68/167 of 18 December, 2013.
[672] Article 17 of ICCPR, (1966).
[673] Sadia Rasool. "Cyber security threat in Pakistan: causes Challenges and way forward." *International Scientific Online Journal*, (2015).

Telenor and other network companies of telecom which are currently working in Pakistan after the promulgation of PECA had adopted this Act in their privacy policy. It is displayed by them that "we operate in a legal framework" and among other policies, the PECA is also mentioned there. However, it is not discussed whether the intrusion and monitoring into one's privacy is the prior condition for obtaining license. Moreover, the MRTTR is also not there under the policies in which they work.[674] These companies don't reveal any provisions in case of hacking of data from cell phones and on their networks. But the Telenor company give some provisions regarding the steps which may be taken for protection of data and information. Although it also does not reveal the demands of government to access or monitor any data.[675]

The instances of women victimization on social groups and internet is very common in Pakistan. They become easy prey of surveillance and monitoring. Females are targeted by different persons for different purposes. Sometimes they are victimized to take revenge from the males of their families. In other instances, these females are extorted for not fulfilling some demands of ill minded peoples. Technology is used to harass them or to access their information shared on social media. There must be specific laws related to the issues of females. Some special laws should be enacted to cater this matter wisely. Deterrence should also be created by making severe punishments in the case of female's victims. A female journalist told in her survey that the females are targeted and monitored by state and non-state actors equally.[676]

Hacktivism is also common on cyberspace. The motivated persons use this skill to danger the data, information or security of any website. The hacktivism technique is usually used in

---

[674] Ibid;
[675] Adnan Chaudhry, "Content Regulation in Pakistan's Digital Spaces June 2018", HRC Report, (2017).
[676] "Surveillance of Female Journalists in Pakistan", Digital Rights Foundation, 31 December, (2016).

political or religious rivals. In this situation a website is hacked and defaced along with the publishing of such material which is against to some political party or religious belief.[677] Pakistan is also facing this dilemma in cyberspace. Political, religious or ethnic groups attack security of a state in this way.

Interception is also taking place across the country. Phone calls and other digital communications are continuously intercepted for the acquisition of data and information. Some interception is conducted by government and its institutions. Unlawful and arbitrary interception is also carried on in Pakistan without any legal justification. It is the matter of concern to distinguish the lawful and arbitrary interception of information and communications. It is also worth mentioning to declare the agencies and institutions whether they are authorized to do interception of the citizen's call. Moreover, the purpose and object of such interception should also be well defined. In 2017, the Human Rights Council has adopted a resolution on the right to privacy in digital age. In this resolution the states are restricted to intervene into the privacy of a person. The interception technologies are prohibited to make the data accessible. However, in Pakistan such ban is ineffective. NSA also spied in Pakistan with the help of malware. The communication intercepted, and metadata gathered by NSA.

It is reported that in Pakistan, ISI tapped the large volume of phone calls ranging between 6,523 phones in February, 6,819 in March and 6,742 in April 2015. This matter came into knowledge in the hearing of a case before Supreme Court. It is also the matter of concern that the phone companies are required to follow the rules of PTA for getting license to operate the said

---

[677] John Arquilla and David Ronfeldt, "Activism, Hacktivism, and Cyberterrorism: the Internet As a Tool for Influencing Foreign Policy", In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, 50. Rand Corporation, (2001).

companies. These rules bound the service providers to intercept and access network data of the users. However, the clear purpose of such interception is not mentioned. Many companies are working in the country to monitor the transferred and communicated data. Government has also installed many technologies for the purpose of surveillance of communications and data. The Center for Advanced Research in Engineering and the National Radio Telecommunication Corporation of Pakistan has also started work with military to monitor the data and calls and to intercept the transmitted data. Foreign companies are also working in Pakistan to provide the technology for surveillance. Trovicor, a German based surveillance technology company and Nokia Siemens Networks (NSN), provided the interception technology to Pakistan. NSN is the first company which provided Global System for Mobile (GSM) network to lawfully intercept the phone calls. Similarly, many other interception technologies and programs are installed by government of Pakistan to monitor the cellular data of citizens which are competing the UK' Tempora and the US' Upstream programs.

Censorship techniques are used to intercept the data and make surveillance. These censorship technologies are used to monitor the terrorist activities, blasphemous material and obscene literature. These same technologies are used to monitor the communication data of the citizens. PTA has also contracted with NARUS an American company to insight the data and emails by inserting packet inspection programs. Pakistan Telecommunication Ltd. (PTCL) also uses deep packet inspection provided by US-based blue coat systems.

Mobile monitoring equipment are used to observe the calls and other data. Many technologies are purchased from Germany, Finland and Swiss companies to make advance techniques for surveillance of mobile communications. In 2013 a report revealed that Finfisher program is

working in Pakistan to infect the data of internet and mobile communications and to gain access to such data. A petition moved by civil liberties to locate the matter. Lahore High Court, ordered the PTA to investigate it but it was not proceeded further. Pakistan also tried to counter the Finfisher. For this purpose, a hacking team was hired from Italy.

Pakistan Government is using various Tactical Communications Surveillance Technologies (TCSTs). IMSI catchers are among of these technologies which are used to make close surveillance of a person's phone calls. These technologies are operating by devices which connect the phones with IMSI catchers rather than mobile phones. It is a threat to the privacy of a person.[678]

This surveillance is maintained without the consent and knowledge of the person. Law enforcement agencies are involved in such type of surveillance. These devices are taken by other countries like Europe, Germany, Italy and America. Similarly, a report exposed that ISI monitored the communication activities through the internet cables in Southern Punjab by installing the surveillance devices. With the help of this monitoring system; the wifi, 3G and internet traffic data could be collected by the ISI. This system was undetectable and unified to the subscribers. Such type of surveillance is a compromise with the right to privacy.[679]

Intrusion malwares are also used to monitor and gather the information data. These malware intrusion techniques are used by government and other companies to watch the activities on internet and mobile phones. From history, it is revealed that finisher, Skynet, and other malwares are used for interception. RCS are used to filter the computers and mobile devices of the people

[678] A. Ahmed and D.S. Khan, "Cyber Security Issues and Ethical Hacking in Pakistan", *Department of Computer Science Karachi University*, (2015).

[679] Z. Ali, M. Jan and A. Iqbal, "Social media implication on politics of Pakistan; measuring the impact of Facebook", *The international Asian research journal,* 1(01), (2013): 13-21.

sometimes with their will under some covered permissions. PTA also blocked access to Virtual Private Networks (VPNs) and amounts the communication illegal and hidden conducted on the basis of using VPNs. In 2015, Blackberry was banned in Pakistan for not allowing interception to its servers. However, later on the blackberry and its messenger stayed in Pakistan after making some agreement with government.

5.4 Challenges for Application and Enforcement Mechanism to Enforce Cyber Laws:

It is the need of hour to make the laws regulating the cyberspace. There must be adequate cyber code of laws and policies. Pakistan is far behind in cyber legislation. Further it is also the responsibility of the Pakistan's government to ensure the privacy as a fundamental right. Privacy has been recognized as a fundamental right in the constitution of Pakistan[680] and various international instruments that has been ratified by the Pakistan. Now it is the duty of courts and legislatures to implement and safeguard this right.

International laws and policies of developed nations may be adopted to design the domestic laws. Pakistan is not sufficient in cyber laws. The cyber strategy and the cyber policy are the need of the time. There should also be the proper enforcement of human rights to shelter the citizens from unjustified intrusions. The privacy of information and data may be assured for the security of both, the state and its nationals. However, some exceptions may be there to the right to privacy.

[680] Article 14 of Constitution of Pakistan, (1973).

These exceptions should be exercised with great cautions. Cyber jurisprudence may be developed to secure the dilemma of cyberspace. Cyber courts should also be made to deal with cybercrimes.

Advanced technologies should be used to investigate the cybercrime and to control the misuse of technology. Pirated software should be completely ban into the country. The state should take initiative to produce the hardware and software into the country. The state should not compromise the other states to spy on the communications of its nationals. Moreover, the independent cybercrimes wings must be opened to deal with cyber threats. The data on government websites and financial institutions be kept save by advanced techniques. There must be heavy punishments for data breaches.

The minorities rights should be saved by the states. The women and children's right to privacy shall be made more secured by imposing heavy penalties on criminals. Education and awareness programs should be conducted on regular basis to make the public aware of cybercrimes. Safety measures should also be taught to the people to secure the data on internet and computers. Implementation and enforcement of domestic laws in the light of international laws is inevitable and remains a big challenge for Pakistan. Followings are some prominent challenges to enforce cyber laws in Pakistan.

5.4.1 National Response Centre for Cybercrime (NR3C) Deals Only with Those Crimes Which are Mentioned in PECA:

To control and counter cybercriminal, Pakistan has established National Response Center for Cybercrime (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 international

institutions and organizations to control crimes originated from Pakistan. It conducts trainings, arrange workshops and seminars for education purpose in cyber domain. It was found that the advancements in technology brought new threats for data privacy in Pakistan. A large number of these innovations were embraced and realized without legitimate assurances, for example, Identity frameworks, the use of computers, internet and social Media, mobile phones etc. This center was established in 2007. It was regulated under the provisions of Prevention of electronic Crimes Ordinance, 2007. This center was the cyber-crime control branch of Federal Investigation Agency (FIA).[681] 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.

This center was made to make the cyberspace free from criminals. Private and public complaint are addressed in this center. However, this center is working only against the offences which are mentioned in the PECA. As it has already been discussed that there are some flaws in the said act. This Act does not provide the clear segregation of rights. Moreover, right to privacy is compromised in this Act. There must be the line, drawn between the right to privacy and the compromising situations in which this right cannot be practiced.

5.4.2 Inadequate Cyber Security Strategy of Pakistan:

As cyberspace has created many dangers to the privacy of 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 the data protection measures. In this regard various strategies may be adopted. To manage these privacy intrusions different authorities may be established by

[681] Usman, Mahboob. "CYBER CRIME: PAKISTANI PERSPECTIVE." *Islamabad Law Review* 1, no. 3 (2017): 18-III.

the government to take necessary actions for the breach and safeguards of privacy. Every sector of a state may be handled by a separate ministry and department so that the information and data may be properly sheltered by independent administration. In this way proper check may be kept on the criminal activities. The authorities may also be accompanied by the secure repositories to record the data in safe hands. Laboratories and investigation techniques may also be exercised to highlight the criminals for offences.[682]

In Pakistan the more focus is exercised towards the protection of military information on cyberspace. Other type of information and data of individuals is not much important. That is the reason many intrusions from national and international cyber criminals have been made to encroach the privacy of other sectors especially the banking sectors. Similarly, kinetic issues of privacy breach are considered of greater significance rather than other non-kinetic issues.[683] Pakistan has two response and security measures to deal with privacy issues in cyberspace. One is the National Response Centre for Cybercrime (NR3C). The other is the Pakistan's Senate Defense Committee.

After revealing the facts by Edward Snowden that Pakistan has been spied by the US National Security Agency (NSA). It is the dangerous situation for Pakistan to remain silent and sedentary in making cyber security policy for the 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.[684] This channel is used to communicate between the

---

[682] Malik, Muhammad Baqir. "Pakistan and India Cyber Security Strategy." *Defence Journal* 17, no. 11 (2014): 59.
[683] Privacy International, "Tipping the scales: Security & surveillance in Pakistan", *Special Report*, July 2015, https://privacyinternational.org/sites/default/files/2018.
[684] Lyon, David. "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique." *Big Data & Society*, (July 2014). https://doi.org/10.1177/2053951714541861.

military and civilian authorities. It is also reported by the Snowden that NSA spied in Pakistan by using a tool known as SECONDDATE. This tool targeted the FOXACID server of Pakistan and collected all desired information from the computer systems.[685] It is also estimated that about 13.5 billion data is interfered including phone calls, faxes, e-mails.[686]

Senator Mushahid Hussain Syed the then chairman of the senate committee arranged a meeting with the Pakistan Information Security Association (PISA) to make negotiation for the development of a cyber security strategy.[687] Many discussions were concluded in this meeting. It was suggested that the funds must be allocated for cybersecurity as it is necessary to protect the cyber attacks in Pakistan. Seven points Action Plan was discussed by the committee.[688] These points are the adoption of the proper legislation for the cyber security.

It was asserted that the cybersecurity is like a terrorism and must be addressed on serious bases by the government. It was also stated that the National CERT should be established to make experts for technical issues in cyberspace. It was further planned that a new task force should be organized for working with various ministries and organizations to promote cyber security of Pakistan and to control cyber threats. It was also suggested that a cyber command center shall also be made for Inter-Services forces to combat the cybercrimes. It was further added that Pakistan should make strategies with the help of other G8 and SAARC countries so that an environment of mutual cooperation may be developed to secure the cyberspace for mutual interests.

---

[685] Haq, Ul, and Qamar Atta. "Cyber Security and Analysis of Cyber-Crime Laws to Restrict Cyber Crime in Pakistan." *International Journal of Computer Network & Information Security* 11, no. 1 (2019).
[686] Baloch, Haroon. "Internet Rights and Legislation in Pakistan: A Critique on Cyber Crime Bill, 2016." *Accessed on 23rd June* (2016).
[687] Senate of Pakistan. "Report of the Senate Committee on Defence and Defence Production," 01 Sep. (2013).
[688] Ibid;

Further, it was also planned that the awareness education shall also be arranged to make the people familiar with the nature of cyberspace and the precautionary measures to protect the information. It was also decided that the cybersecurity policy strategy will be presented by PISA.[689] It was also elaborated that the government and private organizations should work together for the development of a reasonable Cyber Security Strategy. It was further suggested that the industries, economy and citizens will work together to control the cybercrimes. These proposals were forwarded to the National Assembly but unluckily no strategy has been yet drafted to secure the cyber domain.[690] The government should take necessary steps to draft an adequate security strategy to secure the cyberspace. A recent cooperation has been made by the government with the Shanghai Cooperation Organization (SCO) to promote the secure cyberspace.[691] It was also aimed to make such arrangements to tackle the cyber-crime in both countries by joint collaboration.[692]

Pakistan should design its Cyber Security Strategy on emergency basis as it has great threat of cyber warfare. Moreover, the whole economy is dependent on internet therefore the policies should be there to preserve the industries from financial and information losses. Banking industry is also on stake for privacy interference. Many recent examples are there for such intrusions. A few days ago, bankislami experienced the worst cyber attack which resulted into financial loss of

[689] Haq, Ul, and Qamar Atta. "Cyber Security and Analysis of Cyber-Crime Laws to Restrict Cyber Crime in Pakistan." *International Journal of Computer Network & Information Security* 11, no. 1 (2019).
[690] Ibid;
[691] Yamin, Tughral. *Cyberspace CBMs between Pakistan and India*. National University of Science and Technology, 2014.
[692] Yamin, Tughral. *Cyberspace CBMs between Pakistan and India*. National University of Science and Technology, 2014.

2.6 million rupees.[693] Similarly, the websites of important institutions are also hacked and defaced many times. To control these threats there must be a good cyber security strategy and regulations to control and monitor the cyber threats.

5.4.3 Inadequate Security of Critical Information Infrastructure in Pakistan:

The critical information infrastructure (CII) of a country is the most important property of that 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.[694] Critical infrastructure varies from situation to situation. It is the society which decides that what is the critical infrastructure for it. It may be the water supply, energy supply, health service, military services, financial services, telecommunication services, or other government services which may be marked as critical infrastructure of a country.[695]

This infrastructure is directly attached to an information system. If this information system is compromised then the whole critical infrastructure will be threatened and targeted. It is reported by the McAfee, an antivirus software company, revealed in its report that about two third critical infrastructure companies were found infected with highly dangerous malware which were intentionally forwarded to them to target their CI.[696]

---

[693] Cyberattack costs BankIslami Rs2.6m, https://www.dawn.com/news/1422222/cyber-attack-costs-bankislami-rs2m. (Last accessed: 16 November, 2018).

[694] Volkman, Richard. "Privacy as life, liberty, property." *Ethics and Information Technology* 5, no. 4 (2003): 199-210.

[695] Ibid;

[696] Diamond, Jonathan. "Guidelines for the Protection of National Critical Information Infrastructure: How Much Regulation?" 31 July, (2013). [Online]. Available: https://cisindia.org/internet-governance/blog/guidelines-for-protection-of-national-criticalinformation-infrastructure.

Different countries give different values to various infrastructures of their country.[697] But some infrastructure is the common among states which are considered important. In 2016 after the Russian intrusion into US elections, elections had also become critical infrastructure for the country.[698] Critical infrastructures are controlled by the government or various public and private organizations. The most important CI is controlled by the Government itself while the others are given to the various related organizations.[699]

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 CIs exists in Pakistan. Though, in PECA,2016 it is mentioned that whoever will interfere with the critical information infrastructures shall be liable to commit crime. Similarly, it is made more punishable for interferences, alteration, damaging or copying the critical information infrastructures.[700] Further it is also connected to the cyber terrorism. It means that there are some critical infrastructures in the country which contain sensitive information. Moreover, the government is also concerned with the security of these infrastructures. It should be made clear for the proper protection of the state that which infrastructures are critical so that these can be made more secured.

Pakistan is a state which has nuclear power. Because of this nuclear plant and the geographical position of the state it is a continuous threat of cyber attacks on the states to target the information systems of nuclear. It was also reported by Indian hackers that they have made

---

[697] Gercke, Marco. *Understanding Cybercrimes: Phenomena, Challenges and Legal Response*. International Telecommunication Union, 2012.

[698] Fidler, David P. "Transforming election cybersecurity." *Digital and Cyberspace Policy Program, May 2017* (2017).

[699] Zulhuda, Sonny. "Towards a Secure and Sustainable Critical Information Infrastructure (CII): A Study on the Policy and Legal Frameworks in Malaysia." (2010).

[700] Prevention of Electronic Crimes Act 2016, s. 2 (1) (j) & s.6-8.

access to the nuclear infrastructure of Pakistan. It was also asserted by Indian hackers that they have also accessed the military infrastructure of Pakistan.[701] Pakistan also claimed to have targeted various CI sites of the India. Keeping in view these situations of the cyber-attacks there must be decent cyber security measures to control the CI of the country.[702]

5.4.4 Lack of Computer Emergency Response Team (CERT):

Computer Emergency Response Team (CERT) is the composition of high technical professionals. They are qualified to deal with the cybercrimes. These people are well equipped to tackle with the crimes committed on or by computers and internet. They are expert to understand the technology and to find out the source of crime. This team is government based national team to combat computer crimes as it is defined by the European Union Agency for Cybersecurity (ENISA)[703] that CERT is the Government team for national security purpose. This team is qualified with the skills to protect the national cyber security of the country and to secure the critical infrastructure of the state. The team also assists a nation to rehabilitate from a computer attack. It also makes cooperation with foreign countries to help them in crime control or to locate the criminals in the country.[704]

---

[701] Rasool, Sadia. "Cyber security threat in Pakistan: Causes, Challenges and Way forward." *International Scientific Online Journal* 12 (2015): 21-32.

[702] Naureen, Adeela, and Umar Waqar, "Indo Pakistan cyber war: Reality check." *The Nation*, 28 August, (2012).

[703] The European Union Agency for Cybersecurity (ENISA) is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe.

[704] Bada, Maria, Sadie Creese, Michael Goldsmith, Chris Mitchell, and Elizabeth Phillips. "Computer Security Incident Response Teams (CSIRTs): An Overview." *The Global Cyber Security Capacity Centre* (2014).

In Pakistan it was aimed to make a CERT by the Senate defense committee.[705] This team was among the plans to design a cybersecurity strategy of the country. But still there is no CERT in Pakistan. However, National Response Center for Cybercrimes (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. This center works to eliminate the computer frauds, to restore the data damage, to eliminate the cyber threats and the targeted attacks. This center is the branch of the FIA which is the security agency of Pakistan. FIA is regulated by the ministry of Interior of Pakistan.

In the absence of CERT, NR3C is working to deal with cybercrimes in an efficient way. It provides the technical expertise to the government to secure the information and data. It also conducts the digital forensics, mobile forensics, computer forensics, video forensics, security audits and penetration test for intrusion into information. It also entertains the complaints received from the public. It cooperates with the other security agencies to deal with crimes. Forensic expertise is the major ability of this center. The FIA is making efforts to eliminate the cybercrimes from the country. For this purpose, it is intended to hire the technical experts in the ministry so that the personnel of experts may work efficiently to handle cybercrime threats in the country.[706]

Pakistan has also no representation on international level because of non-availability of CERT. NR3C is trying to accomplish the tasks of CERT but it is not the member of "Forums of

[705] Report of the Senate Committee on Defence and Defence Production
http://senate.gov.pk/uploads/documents/1378101374_113.pdf

[706] Ibid;

incident Response of Security Teams (FIRST)"[707], which is a global setup for the registration of CERT of every country. A private team of IT experts is working in the Pakistan with the name of PAK CERT. It was established in 2000 to provide the IT expertise at national level.[708] To create a National CERT a draft was presented in 2014 namely "The National Security Council's Act".[709] But this draft was rejected by the Ministry of Information Technology on the instance that the provisions of the draft are impracticable. It was not the wise decision as the draft could be amended rather than to make it the part of trash. In this proposed Act it was also viewed that a cyber security expert personnel of IT professionals shall also be hired to make the cyberspace secure. This team would be the national CERTs but the Act was not welcomed and rejected because of its insufficiency to address the cyber security issues such as the intrusions into critical infrastructures and unauthorized access to the personal information.

It is announced by The Pakistan Information Security Association (PISA) that they had organized a group of IT professional to deal with cybersecurity issues. This group is called PISA-CERT and it is well equipped with the skills to control and investigate cybercrimes. It is further said by the PISA that it is the National CERT and this is the first public personnel of experts to

---

[707] FIRST is the global Forum of Incident Response and Security Teams. FIRST is the premier organization and recognized global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents reactive as well as proactive.

[708] Pakistan Computer Emergency Response Team (PakCERT).https: www.pakcert.org/aboutus.html (Last accessed: 16 November, 2018).

[709] The National Security Council's Bill ,2014 http: www.senate.gov.pk/en/billsDetails.php?type=1&id=-1&catid=186&subcatid=276&leftcatid=279&cattitle=Bills. Last accessed: 16 November, 2018).

control the cybercrimes. However, no provisions and information are mentioned on the website of PISA in this regard.[710]

Pakistan is far behind from other countries in cyberspace strategies. There are no preventive and remedial steps from the state to protect its cyberspace. No international cooperation is made in this perspective as well. Pakistan is also not the member of international CERT forum. It has not signed any Memorandum of Understanding (MoU) for the security of cyberspace with any other country. Moreover, Pakistan has not signed or ratified the Budapest Convention which is the International convention on cybercrimes.[711]

However, Pakistan is the member of "Asia Pacific Computer Emergency Response Unit" (APCERT) to make cooperation and to deal with cybersecurity threats.[712] Pakistan is also the general member of OICCERT. This CERT is working with the cooperation of OIC members to control the cybersecurity dilemmas and to secure the cyberspace. It is also working for promoting and sharing knowledge and skills on cybersecurity profession. Pakistan is represented in OICCERT by NR3c and PISA-CERT as there is no National CERT in the country.[713]

It is the matter of worth to develop the proper cybersecurity team and cybersecurity strategy not only to control the cyber threats but also to represent the Pakistan at international level. The international policies and strategies should be adopted to make the domestic laws in line with international laws. At national level there must be team of cyber skill experts. A cybercrime

---

[710] Report of "Pakistan Information Security Association." Online available: https://www.pisa.org.pk/. (Last accessed: 16 November, 2018).
[711] Zia, Haleemah, Rabeea Imran, Rahat Masood, and Muhammad Awais Shibli. "Framework for the Development of Computer Emergency Response Team in Pakistan." *NUST Journal of Engineering Sciences* 10, no. 2 (2017): 65-71.
[712] Ibid;
[713] "OIC-CERT Annual Report 2016," 31 Dec. (2016).

division furnished with forensic laboratory and cyber experts may also be attached to each police station.

5.4.5 Lack of Education and Awareness on Cyber Security in Pakistan:

The education on cybersecurity is not efficiently provided in Pakistan. Only some institutions and universities are providing cybersecurity education. Moreover, the education and syllabus are not sufficient to tackle the cybersecurity threats in the countries. Institutions are not playing their role to make the students aware with the knowledge of cybersecurity and information warfare which is a giant threat to the security of a nation. The future perspective of information and cyber warfare is very obvious if sufficient and efficient preventive security measures are not adopted.

It is responsibility of the state and educational institutions to make awareness sessions, seminars, conferences and workshops to update the citizens with adequate knowledge of cyberspace, internet, computer systems and ICTs.[714] The people should be made acquainted with the nature of cyber-attacks and the safety measures to protect their information and data. Education institutions should take initiative to promote the cyber technology education. Some institute provide the educational courses on cyber security but only to the extent of military.[715] The education about computer networks, cybersecurity and information frauds is only provided in military college of signals.[716] The other universities are not making contribution to educate the

---

[714] Syed, Rubab, Ahmed Awais Khaver, and Muhammad Yasin. "Cyber Security: Where Does Pakistan Stand?" (2019).

[715] Ibid;

[716] Shafqat, Narmeen, and Ashraf Masood. "Comparative analysis of various national cyber security strategies." *International Journal of Computer Science and Information Security* 14, no. 1 (2016): 129.

students in computer networking. Only very few universities are giving degree in information technology.[717] Cyber Law are not included even in LL.B syllabus in Pakistan.

In Pakistan there are only few institutes to provide the trainings in information security. These institutes also give certifications like Certified Information System Security Professional (CISSP) awards to the trainees of information security.[718] Some institutions provide the training course on Professional Ethical Hacking.[719] Pak-CERT is providing special training sessions to the corporate customers for security of digital information and preventing hacking. This team is also providing some professional education in the form of CISSP, network forensic, ethical hacking, penetration testing and computer security. It is also updating people to manage the security risks and to recover the damaged data and information.[720]

NR3C also played important role to promote cybersecurity awareness in the country. It arranged different training sessions on the basic information of cyberspace and computer related crimes. It is reported that between the bracket of 2014 to 2017 NR3C has educated almost 12,458 persons from all walks of life about the cyberspace and the threats related to information.[721] Information Security Association Pakistan (PISA) is also participating to make awareness programs to the public to make them acquainted with the nature of cybersecurity and the threats

---

[717] Shad, Muhammad Riaz. "Cyber threat landscape and readiness challenge of Pakistan." *Strategic Studies* 39, no. 1 (2019): 1-19.

[718] Syed, Rubab, Ahmed Awais Khaver, and Muhammad Yasin. "Cyber Security: Where Does Pakistan Stand?" (2019).
[719] Ibid;
[720] Moneeb Junior, "Cyber Secure Pakistan 2018", International Cyber Security Conference held in Islamabad. 29 Mar, (2018).
[721] Ibid;

to the information on cyberspace. It also arranges training sessions and awareness seminars for its professionals.[722]

A conference was also arranged in 2018 with the name "Cyber Secure Pakistan". This conference was arranged to trained the people to manage the security of their information and data on cyberspace. The girls and women were specially educated to handle their privacy on information systems, social media websites and cellular mobile phones. Moreover, they were also introduced with the cyber laws and their rights along with different remedies in case of any damage committed against them on cyberspace.[723]

This small number of institutions delivering the knowledge of computer security and Information, is not sufficient for the population of 200 million people. The other perspectives i.e., cyber warfare, cyber terrorism, security of critical infrastructures etc. of cyber security and cyber threats to information and data privacy are neglected. The critical infrastructures are dependent on the proper safety techniques.[724] The institutions should play their role to secure the critical infrastructure information by developing an approach of cyber awareness. Moreover, the universities should arrange MoU with foreign universities to educate their students in cybersecurity domain. The foreign scholarships and training sessions may also be arranged to prepare the students for cybersecurity knowledge.

---

[722] Shad, Muhammad Riaz. "Cyber threat landscape and readiness challenge of Pakistan." *Strategic Studies* 39, no. 1 (2019): 1-19.

[723] Moneeb Junior, "Cyber Secure Pakistan 2018". International Cyber Security Conference held in Islamabad. 29 Mar, (2018).

[724] Haq, Ul, and Qamar Atta. "Cyber Security and Analysis of Cyber-Crime Laws to Restrict Cyber Crime in Pakistan." *International Journal of Computer Network & Information Security* 11, no. 1 (2019).

5.4.6 Differences in the Application of Domestic and Human Rights Safeguards

Many Human Rights Documents speak about the right to privacy.[725] There is large number of international human rights instruments which protects the privacy of a person. These documents have been discussed in detail under chapter two. The UDHR, the ICCPR, the CRC, the ICMF, and the CDHR are among these documents. Pakistan has ratified many such human rights documents which supports the right to privacy of an individual. These human rights are also applicable on cyberspace. As with the advancement of technologies, the computers and internet generated the cyberspace, which is also a territory and contains much rights to be preserved. In Pakistan, the human rights are supposed to be imposed without any prejudice. The Constitution of Pakistan also favours the right to privacy. This right must be guaranteed in cyberspace by adopting necessary steps.

Pakistan should endeavour to safeguard this right in cyberspace as well. As cyberspace is the new concept of jurisdiction. It must also be secured for the safety of information and protection of communications. UDHR is also ratified by Pakistan. It also provides the protection to the privacy of a person, his communication and his family. The domestic laws should be enacted in consonance of this Magna Carta of human rights. Pakistan has also ratified the ICCPR and the right to privacy is extrinsically embed in the ICCPR. The Cairo Declaration on Human Rights in Islam is also providing the right to privacy of a person. Pakistan is the signatory of this declaration.

According to the UN'HRC, the surveillance and interference with privacy must be lawful.[726] Its further states that the surveillance must be specifically targeted for the well-defined

---

[725] Report of HRW, "Privacy and Human Rights, Overview", (2003).

[726] Volkman, Richard. "Privacy as life, liberty, property." *Ethics and Information Technology* 5, no. 4 (2003): 199-210.

reasons. These reasons may be the security of the state, curbing the unwanted criminal activities or to restrict the freedom of speech on some legal grounds. It is also stipulated that the surveillance should be made only by the authorized person. Such authorization shall be awarded on justified reasons. These authorizations shall be allowed on case to case bases not on general basis. The well-defined reasons and objectives of such surveillance shall be highlighted for monitoring the phone calls or other communication data.[727]

The UN special Rapporteur also directed that the privacy of communications and monitoring of information data is highly objectionable conduct. It is a besmirch of someone's communications and privacy. This surveillance must be allowed on reasonable and legitimate purposes. It must be resorted on exclusive and unavoidable reasons. An independent and impartial judicial authority should be appointed to look after this activity of surveillance.[728]

International human rights law imposes a definite standard to compromise the right to privacy of communications and information. Such standards set a predetermined range of exceptions to legitimate the surveillance of data and information. Such exceptions should also be enacted in the domestic laws to make the monitoring of internet, telephones, fax and computerized information.[729] Being the signatory of ICCPR and other international human rights instruments, it is the duty of Pakistan to fulfill its commitments regarding the right to privacy.[730] Moreover,

---

[727] A Cyber, *Understanding Cybercrime: Phenomena, Challenges and Legal Response.* Geneva: International Telecommunication Unit, (2012): 281.
[728] "Report of the UN Special Rapporteur on Freedom of Expression", (17 April, 2013), UN Doc. A/HRC/23/40, 81.
[729] HRC decision in *Mukong v Cameroon*, UN Doc. CCPR/C/51/D/458/1991 (1994).
[730] Sherwani, Ms Mariam. "The Right to Privacy under International Law and Islamic Law: A Comparative Legal Analysis."

surveillance can only be exercised with express and prominent provisions adopted in domestic legislation.[731] These exceptions shall be adopted for legitimate objects.

Right to privacy is also present in the constitution of Pakistan. Privacy is guaranteed as a premise right in the constitution labelled as the fundamental right. But this right is compromised under some exceptions. Such as Article 08 states that the law enforcing forces are exempted from the jurisdiction of these rights. However, these provisions must be applied with great care and caution with regard to these inconsistencies. Domestic laws shall be drafted under the compliance of international commitments. The states should make efforts to design a harmony with international human rights laws so that the ambiguity may be avoided. The domestic legislation should assist the compliance of human rights.[732]

Investigation for Fair Trial Act, 2013 authorises the state to make surveillance in Pakistan. This Act provides a wide range of monitoring in the name of access to data, phone calls, emails and other computer bases communications. This access is allowed with the warrant of court on reasonable suspicion that a person is involved in the commission of a crime or making a plan to commit an offence. This permission is very vast in nature as it renders the compromise on the right to privacy.[733] It is the duty of court to issue warrant after making itself satisfy that there are reasonable grounds for having such believe of offence and there is genuine need of surveillance to control the crime. [734]

---

[731] Volkman, Richard. "Privacy as life, liberty, property." *Ethics and Information Technology* 5, no. 4 (2003): 199-210.

[732] Hayat 1, Muhammad Aslam. "Privacy and Islam: From the Quran to data protection in Pakistan." *Information & Communications Technology Law* 16, no. 2 (2007): 137-148.

[733] Husain, Waris. "Surveillance and law enforcement: Tools in the fight against terror in a comparative study of the United States and Pakistan." *ILSA J. Int'l & Comp. L.* 21 (2014): 25.

[734] Investigation for Fair Trial Act, 2013.

The Anti-Terrorism Act, 1997[735] authorise the officers to enter search and seizer into the premises of a person and to take the custody of material, substance, property or any article into custody which is believed to be involved into terrorism. The officer is not required to obtain a warrant from the court. Such type of legislation is an impediment for the enforcement of right to privacy under the ambit of International Human Rights.[736]

The PECA, 2016 also makes the privacy of citizens to be compromised in many instances. Moreover, it also permits the federal government to transfer the data to foreign governments. Similarly, the officers may obtain the access to the data without the permission of the court. It is also remarkable to mention that PECA allows the access to the communication's data which is very broader range of privacy infringement. As the communication data is related to the pattern of behaviour and dealings of persons. It also involves the business transactions and professional associations. The European Union's Court of Justice remarked it as the breath compromise to the privacy.[737]

5.4.7 Unsatisfactory Harmony of Domestic Laws with International Law

Cybercrime is not the dilemma of the Pakistan only. Other nations are also facing the gravity and consequences of this crime. As the nature of the cybercrime is the borderless that's why the legislation and other safety measures may be adopted in sequence of the international law. The domestic laws should be drafted after the consideration and due deliberation on international law

[735] Anti-Terrorism Act, (1997).
[736] Husain, Waris. "Surveillance and law enforcement: Tools in the fight against terror in a comparative study of the United States and Pakistan." *ILSA J. Int'l & Comp. L.* 21 (2014): 25.
[737] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland (Judgment of 8 April 2014) ECLI:EU:C: 2014:238.

so that the advanced measures may be adopted to combat the giant of new and advanced technology commonly known as cybercrime.

The cybercrime is the international and cross border crime that's why the international legislation is the guideline for the drafting of update version of cyber legislation. Pakistan is lagging behind for having handsome number of laws on cybercrimes. Developing countries are not the only prey of cyber-attacks the developed nations have also the same concerns, in spite of that they have designed a reasonable cyber law to defeat the cyber-attacks.[738]

To make the developing countries independent in cyber legislation, the International Telecommunication Union ITU provides the guidelines to be adopted. These Guidelines provide the standards for the protection of online transactions and commerce. It helps the member states to draft such legislation which may be beneficial to control the cyber-attacks, design the secured cyberspace and make cooperation with other states. It provides the security measures to protect the IT infrastructures. It has also produced the books to make good understanding of cybercrimes. "Understanding Cybercrime: Phenomena, Challenges and Legal Response"[739] is the work of ITU prepared by Prof. Dr. Marco Gercke to guide the developing countries. United Nations Office on Drugs and crime (UNODC) also generated some writings to help the member states to control the terrorism. "The Use of the Internet for the Terrorist Purpose"[740] and "Comprehensive Study on Cybercrime"[741] are the works of UNODC to provide security measures to control cyber threats.

---

[738] Mohiuddin, "Cyber Laws in Pakistan, 19.: http://supremecourt.gov.pk/ijc/articles/10/5.pdf (Last accessed: 16 November, 2018).

[739] Marco Gercke, *Understanding Cyber crime: Phenomena, Challenges and Legal Response*, Geneva: International Telecommunication Unit, (2012).

[740] "This was prepared for the open-ended intergovernmental expert group on cyber crime, UNODC. However, this has not been formally edited and remains subject to editorial changes".

[741] "The UNODC Commission on Crime Prevention and Criminal Justice to establish, an open-ended intergovernmental expert group".

The UN General Assembly has also adopted many resolutions to cater the threats and dangers in cyberspace. In the resolutions of 55/63[742] and 56/121[743] respectively, the UN General Assembly talked about the elimination of save heavens in cyberspace for offenders. In Resolutions 57/239[744] and 58/199[745], the UN General Assembly requested the member states to make such practices which may be efficient for the security of information infrastructures. In resolution of 65/230, the UN General Assembly required the member states to make cooperation for the exchange of technical experts and technology to make the cyberspace secure.[746] In its resolution 67/189[747], the UNGA encouraged the member states to study the cybercrimes. 69/166[748] the UN resolution was adopted to protect the right to privacy in cyberspace.

The Council of Europe Convention on Cybercrime was adopted to understand the nature of cybercrimes.[749] The Council of Europe Commissioner for Human rights also stressed for the rule of law in digital era.[750] Pakistan should make laws in the line of these documents to protect the cyberspace. The US has also a wide range of laws dealing with cyberspace. The US department of Justice is working with many states to manage the cyber threats. FBI, US Internet Crime Complaint Center (IC3) and National White-Collar Crime Center (NW3C) are working to control

---

[742] A/RES/*55/63*.
[743] A/RES/*56/121*.
[744] A/RES/*57/239*.
[745] A/RES/58/199.
[746] A/RES/65/230.
[747] A/RES/67/189.
[748] A/RES/69/166.
[749] Council of Europe, "Convention on Cybercrime," 24 April, (2018).
[750] Council of Europe, *The rule of law on the Internet and in the wider digital world*, December, (2014).

the cybercrimes.[751] China is also playing great role in combating cybercrimes. It has the well-defined laws and security forces known as cyber police to control cybercrimes.[752]

Two basic treaties, Copyright Treaty of 1996, and Phonograms and Performers Treaty of 1996, were promoted by World Intellectual Property Organization to introduce the new guidelines for property rights on internet. The OECD also forwarded some guidelines to protect the data and information on cyberspace.[753] Laws relating to cyber threats are needed to be updated in Pakistan for security of information and to control the infringement of privacy rights. The developed countries like the USA, Britain, Germany and Canada may be followed to draft the efficient cyberlaws.

Conclusion

From the discussion, it is concluded that in terms of technology and world's development, there are certain traditional as well as non-traditional threats. The non-traditional threats have been gained more importance in 21st century. In this modern era, technological advancement has facilitated the emergence and advert of data privacy in cyberspace. In Pakistan, the cyberspace dilemma is there. This cyberspace dilemma has evolved in the institutions, banks, educational departments, governmental sector, military sector as well as private and public sector. Pakistan is facing a lot of challenges in respect of the use of technology. More efforts and developments are

[751] "Federal Bureau of Investigation (FBI), the United States Secret Service (US Secret Service), the United States Immigration and Customs Enforcement (ICE), the United States Postal Inspection Service, Internet Fraud Complaint Center, the Internet Crime Complaint Centre (IC3), the National White- Collar Crime Center (NW3C) and the Bureau of Alcohol, Tobacco and Firearms (ATF) are the agencies which investigate cyber crimes and related crimes in the US".

[752] Andrejevic, Mark, and Kelly Gates. "Big data surveillance: Introduction." *Surveillance & Society* 12, no. 2 (2014): 185-196.

[753] Ibid;

required for addressing this concern. The personal data of individuals, private and public is not secured fully throughout the country. In Pakistan, to overcome cyberspace challenges, different laws and policies were formulated but there are serious problems in its implementation. The effective implementation of laws is essential for further progress in Pakistan. Efficient and proper cyber laws and data protection codes shall be adopted on emergency basis to meet the needs of digital era. NR3C shall be made effective to control the intrusions into privacy. Likewise, an appropriate cyber security policy shall be drafted to protect the Pakistan from cyber warfare. A CERT shall also be trained to combat the present challenges of cyberspace and threats to informational privacy. Education shall also be disseminated to individuals to protect their personal information on ICTs. Specially the teen ager girls, working women, children and young boys shall be made aware to protect their personal data on digital devices.

Conclusions and Recommendations

Conclusions

From the discussion, it is concluded that the right to privacy in cyberspace is a fundamental human right. In this regard this study has examined the cyberspace laws and privacy in Pakistan as well as at international level. It has analysed the existing legal frameworks and clarified the current situation particularly in Pakistan. In the beginning, relevant literature review on the subject has been reviewed effectively. The study has examined the historical background of cyberspace and highlighted its development, significance of cyberspace technology and the other relevant concepts. It has briefly discussed the information communication and cyber security as well as the issue of cybercrimes. It has argued that due to cyberspace technology various issues arose, such as cyber-crimes threating to individuals and states' cyber security.

Further, the study has overviewed the historical development of right to privacy. It has revealed that the protection of privacy is significant worldwide. The rapid increase of communication technologies has given birth to the threat of fundamental rights and freedom of the citizens particularly with regard to the issue of privacy.[754] The right to privacy has been recognised in various international conventions and instruments, such as, the UDHR, (1948), the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data[755] and the ICCPR, (1966).[756] It has analysed provisions of IHRL in relation to protection of right to privacy by referring all necessary international documents. The provisions of

[754] Sturma, Dieter, Bert Heinrichs and Ludger Honnefelder, "Biometrics: Enhancing Security or Invading Privacy? Executive Summary", Volume 15, Issue 1,383–390, (2009).
[755] Council of Europe, Europe Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data, (1981).
[756] International Covenant on Civil and Political Rights, (1966).

the UDHR are significant for consideration in this respect whereas the provisions of laws of other developed countries are also useful. It has analysed the International laws pertaining to privacy very aptly and revealed that Pakistan is a signatory to nearly all international treaties that consider privacy as a fundamental human right, including the UDHR, ICCPR and CRC. Further, the regional human rights instruments also protect right to privacy, such as, the ACHR, the EU and the CDHR. Right to privacy has also been justified by judicial decisions given by the American Courts, the ECtHR, the Supreme Court of India and the IACHR. It also discussed the concept of privacy in Islam.

Moreover, it has analysed the cyberspace laws of the America, European countries, Australia and Asian countries. It has debated that how these countries among others have achieved a level of control over cyber activities while trying to minimize the negative impact on their societies. By this discussion it is revealed that cyberspace is a threat for all nations if it is not protected effectively and efficiently by states. It has examined the legal framework of different states to make a better understanding of current trends adopted to protect and secure cyberspace and right to privacy. It has also analysed different approaches adopted by developed countries and revealed that protection of privacy at all levels is necessary. The origin of data protection in cyberspace technology has also been discussed. Privacy Regulations adopted by EU, The UN Guidelines on Data Privacy,1990 and the APEC, 2004 principles are discussed to analyse the data protection in cyberspace. It has also discussed the report of UN Special Rapporteur on the right to privacy in cyberspace and the role of South Asian Association for Regional Cooperation (SAARC) to protect privacy in cyberspace.

It has also evaluated the case study of Pakistan. It has discussed cyberspace laws of Pakistan by analyzing relevant legislation, such as, National IT policy and Action Plan (2000), Electronic Transactions Ordinance (ETO) 2002, Prevention of Electronic Crimes Ordinance (PECO) 2007 and 2009, Prevention of Electronic Crimes Act (PECA), 2016 and so on. It has revealed that the legislation for protection of privacy is almost appropriate. However, implementation of such laws is a big challenge. It has also discussed relevant constitutional provisions and Islamic concept related to cyberspace and privacy. It revealed that the Constitution of Pakistan, 1973 recognizes the individual's privacy as an inviolable right by specifically guaranteeing the dignity of citizens, privacy of home, the protection of life, liberty and body as fundamental rights. Further, it has described the reasons and limitations on right to privacy. Pakistan is required to take special measures for protection of right to privacy of Individuals. It has highlighted that terrorism and similar activities are big challenges. As noted by Ben Emmerson QC, the UN Special Rapporteur on counter-terrorism and human rights that; "The hard truth is that the use of mass surveillance technology effectively takes away right to privacy of communications on the internet altogether".[757] Further, it has also established that privacy is a human right that needs protection at all levels in Pakistan.

Chapter five is specific to the case of Pakistani Society. It has discussed the breach of privacy in cyberspace in context to Pakistani society. It has revealed that Pakistan is trying to meet the digital needs of the world. With the advent of internet, 3G/4G technologies and ICTs, Pakistan is doing struggle to make advancements in both, public and private sectors. It is the need of the

[757] Ben Emmerson, "the UN Special Rapporteur on counter-terrorism and human rights, two years after Snowden: protecting human rights in an age of mass surveillance", Executive summary, Report of Amnesty International, (2015).

time to become updated in the field of digital technology. It has also discussed privacy of a person and state practices including domestic surveillance. In this respect, the role of corporations for protection of right to privacy is important for consideration in Pakistan. Corporations may play important role by advertising or designing a mechanism for protection of digital data. It has also discussed foreign surveillance, Government partnerships, the right to privacy and the issue of gender discrimination. Further, it has analysed cybercrimes related to financial matters disturbing the 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 has revealed that Pakistan has to take necessary steps for ensuring privacy at all levels. It has argued for domestication of international laws in Pakistan is essential for protection of privacy rights. However, it is a big challenge to protect right to privacy of individuals. The ultimate aim of this study was to provide an answer to the research question that the right to privacy is important in cyberspace, and in particular to show the link between privacy and data protection, cyber-security and cybercrime in order to protect the human rights of people and individuals at all levels in Pakistan.

Recommendations

From the above discussion the following recommendations are drawn.

A constitutional amendment is required to be inserted into the constitution. In this amendment the right to privacy in cyberspace is needed to be acknowledged. Further, such provisions may be designed as to protect the right to privacy in cyberspace as a fundamental right of a person. Article 14 is not sufficient to protect the privacy in the domain of cyberspace.

Pakistan should design a meaningful and effective policy to secure the data and information of individuals in digital sphere. It may also be designed to meet the constitutional and international obligations, and establish an independent and well-resourced Privacy Commission to ensure the protection of citizen's privacy rights in offline and online spaces. In this regard the practices of other states like USA, Australia, Japan and Germany may also be followed. There is a great need to make such comprehensive policies which may efficiently control the collection, retention, use and transfer of information related to people. A Data Privacy Protection Act may also be adopted by parliament.

Proper security measures should be adopted to maintain and protect the data in various institutions. Further, the flow of information should also be controlled. Information may be transferred only in required situations. The information should be shared with the appropriate authority only. There must be clear rules for the use of such transferred data. The violation of rules may be penalizing with strong and obvious punishments. The people should have adequate opportunities to review the information related to them. They shall have also the right to update the given information. In certain circumstances they shall have option to restrict the further sharing of their information and personal data. The institutions shall seek permission before further dissemination of data about a person. Data protection and security of information must be treated as an important issue. The information and data available on cyberspace are also required to be safeguarded on priority basis. The privacy measures of developed countries like USA, UK, Australia, Germany, China and Japan can be adopted to protect the cyberspace in Pakistan. Such model laws may be followed which are proven beneficial to curb the cybercrimes. Moreover, the EU directives may also be consulted to collect and transfer the information of individuals.

SAARC and member states may recognise the sovereignty of indigenous peoples over data that are about them or collected from them, and which pertain to indigenous peoples, knowledge systems, customs or territories, by always including formalised indigenous developed principles, a focus on indigenous leadership and mechanisms of accountability. Governments' internal sharing of personal data be distinguished in legislation, policies and practices from releasing data to the public as Open Data. There are no relevant regional developments resulting from the SAARC agreements. From the human rights perspective, the development of a full data privacy law in eight member countries would be a considerable step forward, as would the extension of constitutional privacy rights.

The freedom of speech and right to information should be granted under the ambit of certain restrictions. The internet and the other related advancements must be secured from unnecessary intrusions into one's privacy. Such measures should be adopted which may control the use of internet to exercise the freedom of speech. It may be assured that these liberties are not practiced while harming the integrity of the individual, state or national sovereignty.

There must be awareness sessions for individuals so that they may be able to protect their data on online transactions. Such seminars and workshops shall be arranged in which the use of internet and computers are introduced. The people should be given knowledge about the use of digital technologies. Further the online frauds and misuse of information shall also be told to public. The institutions have a responsibility to guide the employees to protect the records on cyberspace. Education shall be given to secure the privacy of personal data and information. Such syllabus should be designed for the students of schools, colleges and universities which contain adequate knowledge about the right to privacy in cyberspace. Cyber laws may also be included in

LL. B syllabus. It must also be taught to students that how a data and information may be protected and prevented from unwanted intrusions into privacy.

There should be such techniques which can be adopted to protect the information on digital devices. Encryption tools should be adopted to secure the data on cyberspace. Such tools should be introduced to the general public as well. Regulatory bodies should arrange training sessions to make people aware about such techniques.

Data and personal information are needed to be secured in all spheres of life. Educational institutions, banking sectors, government institutions are required to be protected from intrusions into privacy. Health records and income tax details are as much necessary to be protected as the records about the financial transactions. In various departments like financial department, there must be special policies to control the information in that domain.

The service providers may also be warned for the abuse of privacy and mishandling of digital information. Such measures shall be taken to aware the ISPs to control the flow of data and information on cyberspace. Heavy penalties shall be imposed to violators. Further, the ISPs shall take such measures to restrict the interferences into privacy and they shall assist the government in identifying such criminals who are committing any cybercrime within their domains.

In the last but not least the original software may be purchased and hardware may be manufactured in Pakistan.

Bibliography

Articles

Ahmad, Mahvish, and Rabia Mehmood. "Surveillance, Authoritarianism and 'Imperial Effects' in Pakistan." *Surveillance & Society* 15, no. 3/4 (2017): 506-513.

Aleem, Yasir, Muhammad Asif, Mohid Khaliq, Iqra Imtiaz, and Muhammad Umair Ashraf. "The Prevention of Electronic Crimes Act 2016 And Shrinking Space for Online Expression in Pakistan." *Al-Qalam* 25, no. 2. (2020): 1-12.

Amoore, L. "Data derivatives: On the emergence of a security-risk calculus for our times". *Theory, Culture and Society,* 28: 2011.

and Transborder Data Flows 2001.

Andrejevic, Mark, and Kelly Gates. "Big data surveillance: Introduction." *Surveillance & Society* 12, no. 2 (2014): 185-196.

Arquilla, John and Ronfeldt, David. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, 50. Rand Corporation, (2001).

Ayofe, Azeez Nureni. "Approach to Solving Cybercrime and Cybersecurity". *International Journal of Computer Science and Information Security.* Vol. 3, No. 1. 2009.

Bada, Maria, Sadie Creese, Michael Goldsmith, Chris Mitchell, and Elizabeth Phillips. "Computer Security Incident Response Teams (CSIRTs): An Overview." *The Global Cyber Security Capacity Centre* (2014).

Bagchi, Kallol and Godwin, Udo. "An analysis of the growth of computer and Internet security breaches". *Communications of the Association for Information Systems.* 12.46 2003.

Bakhsh, Muhammad, Amjad Mahmood, and Israr Iqbal Awan. "A comparative analysis of cybercrime and cyberlaws in Islamic Republic of Pakistan, Kingdom of Saudi Arabia, and the United Arab Emirates." Imam Journal of Applied Sciences 1, no. 1 (2016): 9.

Bell, R.E. "The prosecution of computer crime". *Journal of Financial Crime.* 9(2), 2002.

Bennett, Colin, and David Lyon. "Playing the identity card." *Surveillance, Security and Identification in Global Perspective. New York and London: Routledge* (2008).

Bennett, Colin J. & Raab, Charles. "The Governance of Privacy: Policy Instruments in Global Perspective", 88, *MIT Press*, 2d ed. 2006.

Bhaimia, Sahar. "The general data protection regulation: the next generation of EU data protection." *Legal Information Management* 18, no. 1 (2018): 21.

Blair, Admiral Dennis C. "House Permanent Select Committee on Intelligence". *Annual Threat Assessment.* 111th Congress, 1st session. 2009.

Bocij, Paul and Leroy McFarlane. "Online harassment: Towards a definition of cyberstalking." Prison Service Journal 139. 2002.

Britz, Marjie T. "A New Paradigm of Organized Crime in the United States: Criminal Syndicates, Cyber-gangs, and the Worldwide Web". *Sociology Compass* 2, no. 6. 2008.

Broadhurst, Roderic, and Lennon YC Chang. "Cybercrime in Asia: trends and challenges." In *Handbook of Asian criminology*, pp. 49-63. Springer, New York, NY, 2013.

Cate, Fred H. Dempsey, James X. and Rubinstein, Ira S. "Systematic government access to private-sector data". *International Data Privacy Law.* vol. 2, No. 4. 2012.

Chapman, A and Smith, Russel G. "Controlling financial services frauds, Trends and Issues in Crime and Criminal Justice". 2: 189, *Australian Institute of Criminology,* Canberra. 2001.

Citron, KD and Norton, H. "Intermediaries and hate speech: Fostering digital citizenship for our information age". *Boston University Law Review.* Vol. 91. 2011.

Clarke, Jeremy and Hengartner, Urs. "Panic Passwords: Authenticating under Duress", *School of Computer Science University of Waterloo.* 2008.

Davies, Simon and Hosein, Ian. "Liberty on the Line" in Liberating Cyberspace, Pluto Press, London, 1998.

Dean, Katie. he Epidemic of Cyberstalking. Wired Magazine, January 5, 2000.

Decary-Hetu, David and Dupont, Benoit. "The Social Network of Hackers". *Global Crime* 13, no. 3. 2012. 160-75. doi:10.1080/17440572.2012.702523.

Diamond, Jonathan. "Guidelines for the Protection of National Critical Information Infrastructure: How Much Regulation?". 31 July, 2013. [Online]. Available: https://cisindia.org/internet-governance/blog/guidelines-for-protection-of-national-criticalinformation-infrastructure.

Dombrowski, Stefan C., Karen L. Gischlar and Theo Durst. "Safeguarding Young People from Cyber Pornography and Cyber Sexual Predation: A Major Dilemma of the Internet." *Child Abusive Review* 16 (2007).

Ellison, Louise, and Yaman Akdeniz. "Cyber-stalking: The regulation of harassment on the ınternet." Criminal Law Review. 1998.

Elmaghraby A.S. & Losavio, M.M. "Cyber security challenges in Smart Cities: Safety, security and privacy". *Journal of Advanced Research*, vol. 5, no. 4. 2014.

Etzioni. "A communitarian perspective on privacy", *Connecticut Law Review*. 2000.

Farid, Shahid, M. Alam, G. Qaiser, A. A. U. Haq, and J. Itmazi. "Security threats and measures in E-learning in Pakistan: A review." *Tech J* 22, no. 3 (2017): 98-107.

Fidelie, Laura Woods. "Internet Gambling: Innocent Activity or Cybercrime?" *International Journal of Cyber Criminology* 1 (2009).

Fidler, David P. "Transforming election cybersecurity." *Digital and Cyberspace Policy Program, May 2017* (2017).

Frieden, Jonathan D. and Leigh M. Murray. "The Admissibility of Electronic Evidence under the Federal Rules of Evidence." *Richmond Journal of Law and Technology* 2 (2011).

Galbreth, Michael R. and Mikhael Shor. "The Impact of Malicious Agents on the Enterprise Software Industry." *MIS Quarterly* 3 (2010).

Gandhi, V. Karamchand. "An Overview Study on Cybercrimes in Internet". *Journal of Information Engineering and Applications.* Vol 2, No.1. 2012.

Gavison, Ruth E. "Privacy and limits of law". *The Yale Law Journal.* Vol. 89, No. 3 1980.

Ghauri, Irfan. "Electronic Crimes Act: Cybercrime to be made non-cognisable offence". The Express Tribune.

Godkin, E. L. "The Rights of the Citizen: To his Reputation". Scribner's Magazine. I890.

Goldschmidt, Orly Turgeman. "Meanings that Hackers Assign to their Being a Hacker" *International Journal of Cyber Criminology* 2 (2008).

Grabosky, Peter. "The Global Dimension of Cybercrime." Global Crime 6.1 (2004): 146 - 157.

Greenleaf, G. "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention". *University of New South Wales Faculty of Law Research Series*. 2011.

Greenleaf, Graham. "Five Years of the APEC Privacy Framework: Failure or Promise?". *Comparative & International Law*. 2002.

Guarnieri, Franck, and Eric Przyswa. "Counterfeiting and Cybercrime: Stakes and Challenges." The Information Society 29, no. 4 (2013): 219-26. doi:10.1080/01972243.2013.792303.

Gupta, Rohit K. "An Overview of Cyber Laws vs. Cyber Crimes: In Indian Perspective". Online available at: www.mondaq.com (Last accessed: 20 November, 2018).

Hakim and Rengert, Introduction, in: S. Hakim & G.F. Rengert (eds), *Crime Spillover*, Sage Publications, Beverly Hills. 1989.

Halder, Debarati. "Information technology act and cyber terrorism: A critical review". Academia.edu.

Haq, Ul, and Qamar Atta. "Cyber Security and Analysis of Cyber-Crime Laws to Restrict Cyber Crime in Pakistan." *International Journal of Computer Network & Information Security* 11, no. 1 (2019).

Haque, Jahanzaib. "Developing a Progressive Internet Policy for Pakistan". Policy brief, Jinnah Institute. 2015.

Harcourt, Bernard E., "Judge Richard Posner on Civil Liberties: Pragmatic Authoritarian Libertarian." *University of Chicago Law Review*. Vol. 74, 2007.

Hathaway, Oona A. Crootof, Rebecca Levitz, Philip Nix, Haley Nowlan, Aileen Perdue, William and Spiegel, Julia. "The Law of Cyber Attack". *California Law Review*. 2012.

Hauch, Jeanne M. "Protecting Private Facts in France: The Warren & Brandeis Tort is Alive and Well and Flourishing in Paris". 68 *Tul. L. Rev.* 1219.1994.

Hayat 1, Muhammad Aslam. "Privacy and Islam: From the Quran to data protection in Pakistan." *Information & Communications Technology Law* 16, no. 2 (2007): 137-148.

Henderson Sandra C. and Snyder, Charles A. "Personal information privacy: implications for MIS managers". *Information & Management.* 1999.

Herhalt, John. "Cyber-crime-A growing challenge for governments". *KPMG Issues Monitor,* 8: 1-24. 2011.

Higgins, George E. "Digital Piracy, Self-Control Theory, and Rational Choice: An Examination of the Role of Value" *International Journal of Cyber Criminology* 1 (2007).

Hinduja, Sameer. "Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future." *International Journal of Cyber Criminology* 1 (2007).

Hof, Simone Van Der, and Bert-Jaap Koops. "Adolescents and Cybercrime: Navigating between Freedom and Control." Policy & Internet 3, no. 2 (2011): 51-78. doi:10.2202/1944-2866.1121.

Hoofnagle, Chris. "Big Brother's Little Helpers: How Choice Point and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement". 29 *North Carolina Journal of International Law & Commercial Regulation.* 2004.

Huie, Marsha Cope Laribee, Stephen F. & Hogan, Stephen D. "The Right to Privacy in Personal Data: The EU Prods the US and Controversy Continues". 9 *Tulsa Journal of* 25 *Comp Law L. & Security Review.* 2009.

Husain, Waris. "Surveillance and law enforcement: Tools in the fight against terror in a comparative study of the United States and Pakistan." *ILSA J. Int'l & Comp. L.* 21 (2014): 25.

Irion, "The Governance of Network and Information Security in the European Union: The European Public-Private Partnerships for Resilience (EP3R)," in Gaycken, S., Kruger, J. and Nickolay, B (Eds.), *The Secure information Society*, Berlin: Springer Publ., 2012.

Jaishankar, K. "Sexting: A new form of Victimless Crime?" *International Journal of Cyber Criminology* 1 (2009).

Jalil, Shamsuddin Abdul. "Countering Cyber Terrorism Effectively: Are We Ready To Rumble?". *SANS Institute.* 2003.

John R. Vacca, *Computer Forensics: Computer Crime Scene Investigation,* 2nd ed. Massachusetts: Charles River Media, Inc. Boston, (2005), p241.

Kang, Jerry. "Information Privacy in Cyberspace Transactions". 50 *Stan. L. Rev.* 1241. 1998.

Khan, Muhammad Azam. "The information age and Pakistan". *Criterion.* 2013.

Khan, Talha. "Cybercrimes: Pakistan lacks facilities to trace hackers", The Express Tribune, 1st February, (2015).

Kigerl, Alex Conrad. "CAN SPAM Act: An Empirical analysis" *International Journal of Cyber Criminology* 2 (2009).

Kreimer, Seth F. "Watching the watchers: Surveillance, transparency, and political freedom in the war on terror." *U. Pa. J. Const. L.* 7 2004. p133.

Kundi, Ghulam Muhammad Allah Nawaz and Akhtar, Robina. "Digital Revolution, Cyber-Crimes and Cyber Legislation: A Challenge to Governments in Developing Countries". *Journal of Information Engineering and Applications.* Vol.4, No.4. 2014.

Kundi, Ghulam Muhammad, Bahadar Shah, and Allah Nawaz. "Digital Pakistan: opportunities & challenges." *JISTEM-Journal of Information Systems and Technology Management* 5, no. 2 (2008): 365-390.

Kundi, Ghulam Muhammad. "E-business in Pakistan: Oppurtunities and threats". *Lap-Lambart Academic Publishing.* 2010.

Kuner, Christopher. "An International Legal Framework for Data Protection: Issues and Prospects", 25 *Computer L. & Security Review*. 314. 2009.

Lavranos, Nikolaos. "Regulating Competing Jurisdictions Among International Courts and Tribunals" *ZaöRV* 68 (2008).

Levi, Michael. "Perspectives on Organised Crime: An Overview". *The Harward Journal.* 1998.

Levin, Avner and Nicholson, Mary Jo. "Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground", *UOLTJ.* 2005.

Lewis, James A. "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats". *Center for Strategic and International Studies.* 2002.

Li, Q. and D. Schaub. "Economic Globalization and Transnational Terrorism A Pooled Time-Series Analysis." *Journal of Conflict Resolution*. 48 (2), 2004.

Lodge, J. "Freedom, security and justice: the thin end of the wedge for biometrics?". *Annali dell Institute Superiore di Sanita* 43(1). 2007.

Luiijf, H. A. M. Besseling, Kim Spoelstral, Maartje and Graaf, Patrick de. "Ten National Cyber Security Strategies: A Comparison". TNO, The Hague.

Lyon, David. "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique." *Big Data & Society*, (July 2014). https://doi.org/10.1177/2053951714541861.

Magalla, Asherry and Mbuga, Emmanuel George. "The Power of Judges in Law Making in Tanzania and Its Effects on the Growth of Law in Digital Environment". *academia*.edu, 2013.

Malik, Muhammad Baqir. "Pakistan and India Cyber Security Strategy." *Defence Journal* 17, no. 11 (2014): 59.

Marion, Nancy E. "The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation" *International Journal of Cyber Criminology* 1 & 2 (2010).

Mativat, Francois and Tremblay, Pierre. "Counter-feiting credit cards". *The British Journal of Criminology*. 37(2): 165- 83. 1997.

McAlone, Nathan. "The 15 Companies That Flooded Your Inbox with the Most Email Spam in 2015." Business Insider. 2016. Accessed May 20, 2016. http://www.businessinsider.com/the-companies-who-send-the-most-email-spam-2016-2.

McKenzie and Milner. "Recent Developments in Data Protection". *China Update*, 9 March, 2009.

Min, Kyoung-Sik Chai, Seung-Woan and Han, Mijeong. "An International Comparative Study on Cyber Security Strategy". *International Journal of Security and Its Applications.* Vol.9, No.2. 2015.

Mohamed, Muazzam. "Cyber Security Standards Compliance: A Vital Measure to Critical Infrastructure Protection". *KPMG.* 2015.

Mohiuddin, Zibber. "Cyber Laws in Pakistan: A Situational analysis and Way Forward". *Ceericsson Pakistan*. 2006.

Momein, Fahd Abdul, and Muhammad Nawaz Brohi. "Cybercrime and Internet Growth in Pakistan." Asian Journal of Information Technology 9 (1). 2010.

Monahan, Torin. "The future of security? Surveillance operations at homeland security fusion centers." *Social Justice.* 2010.

Morris, Robert G., Matthew C. Johnson, and George E. Higgins. "The Role of Gender in Predicting the Willingness to Engage in Digital Piracy among College Students." Criminal Justice Studies 22, no. 4 (2009): 393-404.

Paul Szoldra. "The Favorite Method Hackers Use to Take over Computers Just Got Killed by Microsoft." http://www.techinsider.io/microsoft-macros-office-2016-2016-3.

Piazza, James A., and James Igoe Walsh. "Transnational terror and human rights." *International Studies Quarterly* 53, no. 1 2009.

Posner. "The economics of privacy". *The American Economic Review.* 1981.

Poullet, Yves. "Transborder Data Flows and Extraterritoriality: The European Position". *J. Int'l. Com. L. & Tech.* 2007.

Qarar, Shakeel. "Around 10 banks block international payments on debit and credit cards", 06 November, (2018).

Rafi, Muhammad Shaban. "Cyberbullying in Pakistan: Positioning the aggressor, victim, and bystander." *Pakistan Journal of Psychological Research* (2019): 601-620.

Rasch, Mark D. "Criminal law and the internet, in the internet and business: A Lawyer's guide to the emerging legal issues". *International Judicial Review*, 3(1). 1996.

Rasool, Sadia. "Cyber security threat in Pakistan: causes Challenges and way forward". *International Scientific Online Journal.* 2015.

Rege, Aunshul. "What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud" *International Journal of Cyber Criminology* 2 (2009).

Roberts, Lynne. "Jurisdictional and definitional concerns with computer-mediated interpersonal crimes: An Analysis on Cyber Stalking" *International Journal of Cyber Criminology* 1 (2008).

Salifu, Adam. "The impact of internet crime on development". *Journal of Financial Crime*, Vol. 15. Number 4, 2008, pp. 432-443(12)

Schifreen, Robert. Defeating the Hacker: A Non-technical Guide to Computer Security. Chichester, England: Wiley, 2006.

Schwartz, Paul M. "Preemption and Privacy". 118 Yale L. J. 913. 2009.

Shad, Muhammad Riaz. "Cyber threat landscape and readiness challenge of Pakistan." *Strategic Studies* 39, no. 1 (2019): 1-19.

Shaffer, Gregory. "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards". 25 *Yale Journal of International Law*, 2000.

Shafqat, Narmeen, and Ashraf Masood. "Comparative analysis of various national cyber security strategies." *International Journal of Computer Science and Information Security* 14, no. 1 (2016): 129.

Sherwani, Ms Mariam. "The Right to Privacy under International Law and Islamic Law: A Comparative Legal Analysis."

Solove, Daniel J. "Understanding privacy." (2008).

Stimson, Charles, and Andrew Grossman. "How Must America Balance Security and Liberty?" The Heritage Foundation. 2011.

Strickland, Lee Minow, Mary & Lipinski, Tomas. "Patriot in the Library: Management Approaches When Demands for Information Are Received from Law Enforcement and Intelligence Agents". 30 *Journal of College & University Law* 363. 2003.

Strossen, Nadine. "Recent US and Intl. Judicial Protection of Indvidual Rights: A comparative Legal Process Analysis and Proposed Synthesis". 41 *Hastings L.J.* 805 1990.

Sturma, Dieter Heinrichs, Bert and Honnefelder, Ludger. "Biometrics: Enhancing Security or Invading Privacy? Executive Summary". Volume 15, Issue 1. 2009.

Syed, Rubab, Ahmed Awais Khaver, and Muhammad Yasin. "Cyber Security: Where Does Pakistan Stand?" (2019).

Tribbensee, Nancy. "Privacy and Security in Higher Education Computing Environments after the USA Patriot Act". 30 *Journal of College & University Law*. 2004.

Volkmann, Richard. "Privacy as life, liberty, property", 5th ed. Hingham: *Kluwer Academic Publishers*. 2003.

Wall, David. Cybercrime: The Transformation of Crime in the Information Age. Cambridge: Polity, 2007.

Walia, Ivneet Kaur. "Infringement of Right to Privacy as a Crime." *Available at SSRN 1591081* (2010).

Walt, S.M., The Renaissance of Security Studies. International Studies Quarterly, 1991. 35(2).

Warren, Samuel and Brandeis, Louis. "The Right to Privacy". *Harvard L.R.* 193. 1890.

Weimann, Gabriel. Terror on the Internet: The New Arena, the New Challenges. Washington, D.C.: United States Institute of Peace Press, 2006.

Weismann, Miriam F. Miquelon. "The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?." *The John Marshall Journal of Information Technology & Privacy Law* 2 (2005).

Wolfers, A., National Security as an Ambiguous Symbol. Political Science Quarterly, 1952. 67(4).

Yassir, Ammar and Nayak, Smitha. "Cybercrime: A threat to Network Security". *International Journal of Computer Science and Network Security.* Vol.12 No.2. 2012.

Young, Kimberly. "Understanding Sexually Deviant Online Behavior from an Addiction Perspective" *International Journal of Cyber Criminology* 1 (2008).

Yusuff, Abdulwasiu Ojo Akorede. "Legal Issues and Challenges in the Use of Security (CCTV) Cameras in Public Places: Lessons from Canada." *Sri Lanka J. Int'l L.* 23 (2011): 33.

Yu, Szde. "Fear of Cyber Crime among College Students in the United States: An Exploratory Study" *International Journal of Cyber Criminology* 1 (2014).

Zaheer, Muhammad. "Territorial Jurisdiction on Cyber Defamation in Pakistan's Perspective." *Corporate Law Decisions, Journal Section* (2011).

Zhang, Yanping, Yang Xiao, Kaveh Ghaboosi, Jingyuan Zhang, and Hongmei Deng. "A Survey of Cyber Crimes." Security and Communication Networks Security Comm. Networks 5, no. 4 (2011): 422-37. doi:10.1002/sec.331.

Zia, Haleemah, Rabeea Imran, Rahat Masood, and Muhammad Awais Shibli. "Framework for the Development of Computer Emergency Response Team in Pakistan." *NUST Journal of Engineering Sciences* 10, no. 2 (2017): 65-71.

Zulhuda, Sonny. "Towards a Secure and Sustainable Critical Information Infrastructure (CII): A Study on the Policy and Legal Frameworks in Malaysia." (2010).

Books

Alberts, David S. and Papp, Daniel S. *The Information Age: An Anthology on Its Impact and Consequences.* CCRP Publication Series. 1997.

Ali, Maulana Muhammad. *Holy Quran.* Ahmadiyya Anjuman Ishaat Islam Lahore USA, 2011.

Anastasi, Joe. *The New Forensics Investigating Corporate Fraud and the Theft of Intellectual Property.* New Jersey: John Wiley & Sons, Inc., Hoboken, 2003.

Baggili, Ibrahim. *Digital Forensics and Cyber Crime.* New York: Springer, 2011.

Bamford, James. *The Puzzle Palace.* Penguin Books. 1981.

Banisar and Davies, The Code War, Index on Censorship, ISSN: 0306-4220 Online ISSN: 1746-6067, sage publications, Volume 27 Issue 1, January (1998) pp. 162–168.

Banks, Michael A. *On the Way to the Web the Secret History of the Internet and Its Founders.* New York: Springer-Verlag Inc., 2008.

Black's Law Dictionary, Ist edition.

Brenner, Joel. *America in the Vulnerable inside the new threat Matrix of Digital Espionage, Crime and Warfare.* New York: Penguin Group Inc., 2011.

Casey, Eoghan. *Digital Evidence and Computer Crime Forensic Science, Computers and the Internet.* 3rd ed. California: Elsevier Inc, 2011.

Christodonte-II, Marcos. *Cyber Within: A Security Awareness Story and Guide.* (Cyber Crime &Fraud Prevention) proactive Assurance LLC. 2010.

Clarke, Richard A. and Knake, Robert. *Cyberwar: The Next Threat to National Security & What to Do About It.* ECCO, 2010.

Dempsey, Gillian Grabosky, Peter and Smith, Russel G. *Electronic theft: Unlawful acquisition in cyberspace.* Cambridge University Press, Cambridge. 2001.

Etzioni, A. *The Limits of Privacy.* Basic Books, New York. 1999.

Gillespie, Alisdair A. *Cybercrime: Key issues and debates*. Routledge, 2015.

Gottschalk, Petter. *Policing Cyber Crime.* Hershey: Petter Gottschalk & Ventus Publishing Aps. 2010.

Grabosky, Peter N. and Smith, Russel G. *"Crime in the digital Age: Controlling telecommunications and cyberspace illegalities".* Federation Press, Sydney/Transaction publishers. 1998.

Grabosky, Peter. *Electronic Theft: Unlawful Acquisition in Cyberspace.* Cambridge University Press. 2001.

Graham, Stepehen Brooks, John and Heery, Dan. *Towns on the Television: Closed Circuit TV in British Towns and Cities.* Centre for Urban Technology. 1995.

Grare, Frédéric. *Reforming the Intelligence Agencies in Pakistan's Transitional Democracy.* Washington, DC: Carnegie Endowment for International Peace, 2009.

Gutwirth, Serge, Ronald Leenes, Paul De Hert, and Yves Poullet, eds. *European data protection: coming of age.* Springer Science & Business Media, 2012: 6.

Hadnagy, Christopher. *Unmasking the Social Engineer: The Human Element of Security.* Wiley; 1 edition. 2014.

Halder, Debarati and Jaishankar, K. *Cyber Crime and the Victimization of Women: Laws, Rights and Regulations.* Hershey: Information Science Reference. 2012.

Heickero, Roland. *"The Dark Sides of the Internet: On Cyber Threats and Information Warfare".* 2012.

Imam Abu Da'ud Book 41, Number 5155.

Imam Abu Da'ud Book 8, Number 1480.

Imam Muslim Book 025, Number 5366.

Jaishankar, K. and Natti Ronel. *Global Criminology Crime and Victimization in a Globalized Era.* New York: CRC Press, 2013.

James, Lance. *Phishing Exposed.* Syngress; 1 edition. 2006.

John Naughton, *A Brief History of the Future The origins of the Internet,* Orion Books Ltd, London, (2001).

Kahn, David. *The Code Breaker the Comprehensive History of Secret Communication from the Ancient times to the Internet.* New York: The New American Library, Inc., 1973.

Lab, Steven P. *Crime Prevention: Approaches, Practices and Evaluations.* Routledge Publishers. 1990.

Li, Chang-Tsun. *Handbook of Research on Computational Forensics, Digital Crime, and Investigation: Methods and Solutions*. New York: IGI Global, 2010.

Lininger, Rachael and Vines, Russell Dean. *Phishing: Cutting the Identity Theft Line*. Indianapolis, IN: Wiley Pub. 2005.

Mali, Prashant. *A Text Book of Cyber crime and Penalties.* (Indiana: Repressed Publishing LLC. 2006.

Mali, Prashant. *A Text Book of Cyber crime and Penalties.* 2008.

Manley, Anthony D. *The Elements of Private Investigation An Introduction to the Law, Techniques, and Procedures.* New York: Taylor and Francis Group, LLC, 2010.

Marcella, Albert J. and Doug Menendez. *Cyber Forensics A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes.* 2nd ed. New York: Auerbach Publications, 2008.

Marcella, Albert J. and Robert S. Greenfield. *Cyber Forensics-A field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*. New York: Auerbach Publications, 2002.

Marvin, Carolyn. *When Old Technologies Were New: Implementing the Future.* Sage Publications, New York. 1999.

Moor, J. H. *The Ethics of Privacy Protection.* Library Trends 39(1 and 2). 1990.

Nyazee, Imran Ahsan Khan. *Legal Research and Writing in Pakistan.* Lahore: Federal Law House, 2014.

Parker, Donn B. *"Fighting Computer Crime: For Protecting Information"*. John Wiley, USA, 1998.

Pedneault, Stephen. *Fraud 101Techniques and Strategies for Understanding Fraud.*3rd ed.New Jersey: John Wiley & Sons, Inc., 2009.

Philipp, Aaron, David Cowen and Chris Davis. *Hacking Exposed Computer Forensics*. 2nd ed.New York: McGraw-Hill, 2010.

Regan, Priscila M. *Legislating privacy: Technology, social values, and public policy*. Chapel Hill, The University of North Carolina Press. 1995.

Reyes, Anthony. *Cyber Crime Investigations Bridging the Gaps between Security Professionals, Law Enforcement, and Prosecutors*. Rockland: Syngress Publishing, Inc, 2007.

Richards, Sally. *Future Net the Past, Present, and Future of The Internet as Told by Its Creators and Visionaries*. New York: John Wiley & Sons, Inc., 2002.

Schifreen, Robert. *Defeating the Hacker : A non-technical guide to computer security.* Wiley., 2006.

Schuler, Karen. *E-discovery: Creating and Managing an Enterprise wide Program A Technical Guide to Digital Investigation and Litigation Support*. Burlington: Syngress Publishing, Inc., Burlington, 2009.

Shah, Aaushi and Ravi Srinidhi. *A to Z of Cyber Crime*. Pune: Asian School of Cyber Laws, 2012.

Shalhoub, Zeinab Karake and Sheikha Lubna Al Qasimi. *Cyber Law and Cyber Security in Developing and Emerging Economies*. Massachusetts: Edward Elgar Publishing, Inc., 2010.

Shaw, Malcolm. N. *International Law*. 6th ed. New York: Cambridge University Press, 2008.

Soma, Madhava P. Sundaram and Umarhathab, Syed. *Cyber Crime and Digital Order*. K. Jaishankar. 2011.

Stephenson, Peter. *Investigating Computer-Related Crime a Handbook for Corporate Investigators*. New York: CRC Press LLC, 2000.

The Holy Quran, Surat-Al-Noor, 24:27-28.

The Holy Quran, Surat-Hujuraat, 49:12.

Torr, James D. *The Information Age.* Greenhaven Press. 2003.

Vacca, John R. *Computer Forensics: Computer Crime Scene Investigation*. 2nd ed. Massachusetts: Charles River Media, Inc. Boston, 2005.

Wall, David. *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge: Polity. 2007.

Wilson, Janet K. *The Praeger handbook of victimology*. California: ABC-CLIO, LLC, Santa Barbara, 2009.

Yamin, Tughral. *Cyberspace CBMs between Pakistan and India*. National University of Science and Technology, 2014.

Yar, Majid. *Cyber Crime and Society.* London: SAGE Publications Ltd. 2006.

Case Laws

1994 SCC 632.

A/RES/45/158 25 February (1991), Article 14.

Acmanne and others v. Belgium, 10 December, (1984), Admissibility Decision, Application No. 10435/83.

AIR 1963 SC 1285

AIR 1997 SC 568.

Amer. Law Reg. N. S. I (1869); I2 Wash. Law Rep. 353 (1884); 24 Sol. J. & Rep. 4(1879).

Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda) 1 July 2000.

Case Concerning Delimitation of the Maritime Boundary on the Gulf of Maine Area Judgement 12 October 1984.

Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits) 27 June 1986.

Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Bosnian Genocide Case) Judgement (Merits) 26 February 2007.

Case Concerning the Application of the Convention on the Prevention and Punishment of

Case Concerning the Land and Maritime Boundary between Cameroon and Nigeria (Cameroon v Nigeria) Judgement (Merits) 10 October 2002.

City of Indianapolis v. Edmond, 531 U.S. 32 (2000).

Dudgeon v. the United Kingdom, 22 October, (1981), Application No. 7525/76. See also *Mosley v. The United Kingdom*, 10 May, (2011), Application No. 48009/08.

Elsholz v. Germany, 13 July, (2000), Application No. 25735/94.

Entick v. Carrington, 1558-1774 All E.R. Rep. 45.

European Court of Human Rights, Case of Klass and Others: Judgement of 6 September 1978, Series A No. 28 (1979). Malone v. Commissioner of Police, 2 All E.R. 620. 1979. Court of

Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014, paras. 26-27, and 37.

European Court of Human Rights, *Weber and Saravia v. Germany*, para. 78; *Malone v. UK*, para. 64.

Ferguson v. City of Charlestown, 532 U.S. 67 (2000).

Gaskin v. United Kingdom, 7 July, (1989), Application No. 10454/83, paras. 41 and 49.

Genocide Case) Judgement (Merits) 26 February 2007.

Ghulam Hussain vs. Additional session Judge, Dera Allah Yar, (2010 PLD 21)

Government of Pakistan, "The National Database and Registration Authority Ordinance, (2000).

Govind v. State of Madhya Pradesh & Anr (1975), SCR (3) 946.

Griswold v. Connecticut, 381 U.S. 479 (1965).

Halford v United Kingdom, (Application No 20605/92), 24 EHRR 523, 25 June, 1997.

Halford v. the United Kingdom, 25 June, (1997), Application No. 20605/92, para. 44.

Handyside v. the United Kingdom, para. 48.

Human Rights Committee decision in *Mukong v Cameroon*, UN Doc. CCPR/C/51/D/458/1991 (1994).

Hunter v. Southam, 2 S.C.R. 145, 159-60 (1984).

Iordachi and Others v. Moldova, 10 February, (2009), Application No. 25198/02.

Jamat-i-Islami Pakistan v. Federation of Pakistan, (PLD 2000 SC 111).

Jeanne M. Hauch, Protecting Private Facts in France: The Warren & Brandeis

Joined Cases C-293/12 and C-594/12 Digital Rights Ireland (Judgment of 8 April 2014) ECLI:EU:C:2014:238.

Judgement of 26 March 1987 (Leander Case).

Katz v. United States, 386 U.S. 954 (1967).

Kharak Singh v. State of UP, 1 SCR 332 (1964).

Klass v. Germany, para. 42.

Kruslin v. France, 24 April, (1990), Application No. 11801/85, para. 33. para. 62.

Kyllo v. United States, 533 U.S. 27 (2001).

Marion Manola v. Stevens & Myers, N. Y. Supreme Court "New York Times " of June 15, I8, 2 I, (1 890).

Mehram Ali v. Federation of Pakistan, (PLD 1998 SC 1445).

Mohtarma Benazir Bhutto and Others vs. President of Pakistan and Others, (PLD 1998 SC 388).

NAACP v. Alabama, 357 U.S. 449 (1958).

Olmstead v. United States, 277 U.S. 438 (1928).

Ople v. Torres, G.R. 127685, July 23, 1998

Pakistan Tobacco Co. Ltd. vs. Government of NWFP, (PLD 2002 SC 460).

People's Union for Civil Liberties (PUCL) v. Union of India and Anr. (1997) 1 SCC 301.

PLD 1993 SC 473

Prevention of Electronic Crimes Act August, (2016).

R. Rajagopal v. State of Tamil Nadu (1994) 6 SCC 632.

Reno v. Condon, 528 U.S. 141 (2000)

Roe v Wade (1972) 410 U.S. 113.

S.P. Gupta vs. Union of India, (AIR 1982 SC 149).

Shariq Saeed vs. Mansoob Ali khan, 2010 YLR 1647 Karachi-High-Court-Sindh.

States v. Miller, 425 U.S. 435.

the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Bosnian

The Rachel affaire. Judgment of June 16, 1858, Trib. pr. inst. de la Seine, 1858 D.P. III

Tort is Alive and Well and Flourishing in Paris, 68 Tul. L. Rev. 1219 (May 1994).

Waris Mesah v. State, (PLD 1975 SC 157).

Whalen v. Roe, 429 United States 589 (1977).

X v. Iceland, 5 Eur. Commín H.R. 86.87(1976).

Conventions

Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems.

Convention for the Protection of Human Rights and Fundamental Freedoms Rome, 4.XI. (1950).

Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data Convention, ETS No. 108, Stasbourg, 1981.

Council of Europe, "Convention on Cybercrime," 24 April, (2018).

Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows 2001.

Council of Europe, Convention for the Protection of Human Rights and Fundamental

Council of Europe, Convention for the Protection of Individuals with Regard to Automatic

Council of Europe, Convention on Cybercrime 2001.

Council of Europe, Draft Modernized Convention for the Protection of Individuals with Regard to Automatic Processing of Individual Data 1981.

Council of Europe, Europe Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data, 1981.

Council of Europe. Additional protocol to the convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS 189). 2003.

Directives

Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 OJ (L 281/). The Data Protection Directive is currently in the process of review, A Comprehensive Approach on Personal Data Protection in the European Union, COM 609, 2010.

Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (Directive 97/66/EC of the European Parliament and of THE COUNCIL of 15 December 1997). <http://www2.echo.lu/legal/en/dataprot/protection.html>. (Last accessed: 20 November, 2018).

EC Council Directive 94/46EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data (Privacy Directive), O.J.L. 281, 1995.

EC, Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and the Council on the adequacy of protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US department of Commerce, O.J. L. 215/007, (2000).

OECD, Guidelines governing the Protection of Privacy and Transborder Data Flows of Personal Data, Paris. 1981.

Pakistan Telecommunication Authority, Directive No.17-1/2010/ Enf/PTA(VPN) Ref: PTA's Monitoring and Reconciliation of Telephony Traffic Regulations, (2010).

Encyclopedias

Encyclopedia of Cybercrime. eds. Samuel C. and McQuade (Westport: Greenwood Press, 2009).

Encyclopedia of Cybercrime. Greenwood Press London. 2009.

Encyclopedia of White-Collar & Corporate Crime. Sage Publications, Inc. Thousand Oaks, California. 2005.

News Channels and Newspapers

Barton Gellman and Ashkan Soltani, "NSA tracking cellphone locations worldwide: Snowden documents show", Washington Post, 4 December, (2013).

BBC News, "Pakistan child sex abuse: Seven arrested in Punjab", (2015). http://www.bbc.com/news/world-asia-33843765 (Last accessed: 16 November, 2018).

Canadian Press, "Police Don't Know if Information Taken from Recovered Hard Drive," CBC News, 2 February, (2003).

Currier, Cora Greenwald, Glenn and Fishman, Andrew. "US government designated prominent Al Jazeera journalist as member of Al Qaeda". The Intercept, 8 May, 2015.

Daily Pakistan, "Another organized child abuse ring discovered in Pakistan, hundreds of photos and videos recovered", (2016). https://en.dailypakistan.com.pk/headline/organized-child-abuse-jolts-khyber-pakhtunkhwa/ (Last accessed: 16 November, 2018).

Dawn, "After Peshawar: Reassessing the terror threat", 18 December, (2014). http://www.dawn.com/news/1151616 (Last accessed: 16 November, 2018).

Gellman, Barton and Soltani, Ashkan. "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say". Washington Post, 30 October, 2013.

Jamal Shahid, 'Flawed' Cybercrime Bill Approved, Dawn News, 17 April, (2015).

Siddiqui, Salman. "Banks being hit by cyber attacks: FIA", The Express Tribune, 7 November, (2018).

The Dawn, "Customer 32 — who used FinFisher to spy in Pakistan?", (2014). https://www.dawn.com/news/1127405. (Last accessed: 16 November, 2018).

The Dawn, "FIA to go after 'corrupt' Nadra officials", (2015). https://www.dawn.com/news/1180042 (Last accessed: 16 November, 2018).

The Dawn, "First child convicted in KP of pornography", (2013). https://www.dawn.com/news/1031509 (Last accessed: 16 November, 2018).

The Dawn, "Hacking Team hacked: The Pakistan connection, and India's expansion plan", (2015). https://www.dawn.com/news/1196767. (Last accessed: 16 November, 2018).

The Dawn, "High tech surveillance system to be launched in Islamabad" (2014). https://www.dawn.com/news/1108273 (Last accessed: 16 November, 2018).

The Dawn, "Pakistani telecoms' murky policies put users' privacy at risk: report", (2016). https://www.dawn.com/news/1305364 (Last accessed: 16 November, 2018).

The Dawn, "preparing pakistan for a cyber war", 17 October, (2012).

The Express Tribune, "Blasphemy: IHC directs authorities to block all social media if necessary", (2017). https://tribune.com.pk/story/1348784/ ihc-directs-authorities-block-social-media-necessary/ (Last accessed: 16 November, 2018).

The Express Tribune, "Chilas town: Saving 'honour' or family riche", (2017). https://tribune.com.pk story/576737 chilas-town-saving-honour-or-family-riches (Last accessed: 16 November, 2018).

The Express Tribune, "Kohistan 'honour' killing: Four years on, no justice in sight", (2016). https: tribune.com.pk story 1034553 kohistan-honour-killing-four-years-on-no-justice-in-sight (Last accessed: 16 November, 2018).

The Intercept. "IMSIs identified with KI data for Network Providers Jan10-Mar10 Trial". National Security Agency, 19 February, (2015.

The Nation. "Pakistani right cries 'blasphemy' to muzzle progressives", (2017). http: nation.com.pk national 17-Jan-2017 pakistani-right-cries-blasphemy-to-muzzle-progressives (Last accessed: 16 November, 2018).

The Nation. "Put blasphemers on Exit Control List,' IHC tells govt". (2017). http://nation.com.pk national 08-Mar-2017 put-blasphemers-on-exit-control-list-ihc-tells-govt (Last accessed: 16 November, 2018).

The New York Times. "Pakistani Says He Killed 3, Using Gay Site to Lure Them", (2014). https://www.nytimes.com/2014/04/29 world/asia pakistani-man-confesses-to-using-gay-sites-to-lure-victims.html?_r=0 (Last accessed: 16 November, 2018).

Statutes

A/HRC/14/46, annex, practice 20.

Anti-Counterfeiting Amendments Act of 2004

Anti-Money Laundering Act, 2010

Article 02 of The Prevention of Anti-National Activities Act, (1974).

Article 03 of Security of Pakistan Act, (1952).

Article 05 of Terrorism Act, (1997).

Article 05 of The Telegraph Act, (1885).

Article 08 of Press Council Pakistan Ordinance, (2002).

Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms

Article 12 of UDHR, (1948).

Article 12 of United Nations' Universal Declaration of Human Rights, 1948.

Article 16(1) of Convention on the Rights of Child, (1989).

Article 17 of Arab Charter on Human rights, (1994).

Article 17 of ICCPR, (1966).

Article 18 of Cairo Declaration on Human Rights in Islam.

Article 2 (1)(a) of West Pakistan Regulation and Control of Loudspeakers and Sound Amplifiers Ordinance, (1965).

Article 3 of the Defamation Ordinance, (2002).

Article 33 of Banking Companies Rules, (1963).

Article 54 of National Security Act, (1947).

Article 8, Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11, Council of Europe (1950–1998).

Associated Press of Pakistan Corporation Ordinance, 2002

Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, (1982).

CCPR/C/21/Rev.1/Add.9, paras. 11 – 16.

Code of Criminal Procedure, 1898

Constitution Act UK, (1867).

Constitution of the Islamic Republic of Pakistan, 1973

Copyright Ordinance, 1962

Data Protection Act, 1978.

Electronic Media Regulatory Ordinance, 1997

Electronic Transactions Ordinance, 2002

Federal Investigation Agency Act, 1974

Freedom of Information Ordinance, 2002

International Covenant on Civil and Political Rights, 1966.

Investigation for Fair Trials Act, National Assembly of Pakistan, 22 February, (2013).

Pakistan - Freedom of Information Ordinance, (2002).

Pakistan Electronic Media Regulatory Authority (PEMRA) Ordinance, 2002

Pakistan Penal Code 1860

Pakistan Telecommunication (Re-organisation) Act, 1996

Patents Ordinance, 2000

Personal Information and Electronic Documents Act (PIPEDA), 2001.

Prevention of Electronic Crimes Ordinance, 2009

Registered Designs Ordinance, 2000

SAARC Charter, 8 December, (1985)

Schedule 02 of PTA Telecommunication Rules, (2000).

Section 05 the Freedom of Information Ordinance, (2002).

Section 08 of Prevention of Gambling Act, (1977).

Section 10 of an Investigation of fair trial Act, (2013).

Section 20 of Control of Narcotics Substance Act, (1997).

Section 25 of the Arms Act, (1878).

Section 32 of Pakistan Telecommunication Act, (1996).

Section 5 of Pakistan Medical & Dental Council Code of Ethics

The Cable Communications Policy Act.

The Children's On-line Privacy Protection Act of 1998 (COPPA).

The Driver's Privacy Protection Act, 1994.

The Fair Credit Reporting Act (FCRA), 1970.

The Family Educational Rights and Privacy Act (FERPA), 1974.

The Financial Modernization Act, 1994.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The Identity Theft and Assumption Deterrence Act.

The Patriot Act.

The Payments Systems and Electronic Fund Transfers Act 2007

The Prevention of Electronic Crimes Act (PECA), (2016) (Act No.XL of 2016).

The Prevention of Electronic Crimes Ordinance, 2007

The Prevention of Electronic Crimes Ordinance, 2009

The Right to Financial Privacy Act.

The Telecommunications Act of 1996.

The Telegraph Act, 1885

The USA PATRIOT Act which was passed on 26th October 2001 (an acronym for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism).

The Videotape Privacy Protection Act.

The Wireless Telegraphy Act, 1933

Trade Marks Ordinance, 2001

Reports, Documents and Working Papers

A Draft Commentary on the Council of Europe's Convention on Cybercrime, October 2000, online available at www.privacy.openflows.org/pdf/coe_analysis.pdf (Last accessed: 20 November, 2018)

A Report of the CSIS Commission on Cybersecurity for the 44th Presidency (Washington, D.C. 2008). Report of ID hacker who store 485000 credit cards Number, prepared by Lehman B. Fed, in info World daily news, World Media Group, 2000.

A. Agha, "Social Capital in Village Organization SadaatHackra, Miani. Bahawalpur, Punjab," 01 April, (2015).

Adnan Chaudhry, Content Regulation in Pakistan's Digital Spaces: June 2018 Human Rights Council Report, (2017).

Ahmed Raza Naseer, "Front Line Defenders", https://www.front-linedefenders.org/en/profile/ahmed-razanaseer (Last accessed: 16 November, 2018).

An International Survey of Privacy Laws and Developments. Electronic Privacy Information Center and Privacy International, US, Electronic Privacy Information Center and Privacy International (2007). Privacy and Human Rights 2006. Online available and retrieved from: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559458, (Last accessed: 20 November, 2018).

APWG, (2013), Phishing Trends Report for Q2. 2013.

Australian Government Report on "Cyber Security Strategy". 2009.

Banisar, David, and Simon Davies. "Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments." *J. Marshall J. Computer & Info. L.* 18 (1999): 1.

Ben Emmerson, the UN Special Rapporteur on counter-terrorism and human rights, Two years after Snowden: protecting human rights in an age of mass surveillance, Executive summary, Report of Amnesty International, (2015).

Biometric Information Technology Ethics, Biometrics and Privacy. Report of the Second BITE Scientific Meeting, Tuesday 26th April 2005, Rome, Italy, (2005), p13. Online available and retrieved from: http://www.biteproject.org/documents/report_biometrics_privacy.pdf, (Last accessed: 20 November, 2018).

Brief amici curiae of Mary Robinson, Amnesty International U.S.A, Interights, the Lawyers Committee for Human Rights, and Minnesota Advocates for Human Rights, Human Rights Watch, Online available and retrieved from: http://www.hrw.org/press/2003/07/amicusbrief.pdf. (Last accessed: 16 November, 2018)

Bytes for All Pakistan and APC, "Safe City Project or Mass Digital Surveillance?", (17 November, 2015). https://content.bytesforall.pk/node/181 (Last accessed: 16 November, 2018).

Bytes for All Pakistan, "Pakistan's Internet Landscape", November, (2013).

Bytes for All, "Gender Tech & Privacy Event", (Feb 17, 2016).

Bytes for All, Pakistan, "Case Studies - Technology Driven Violence Against Women", (2014). http://content.bytesforall.pk/CaseStudies-TechnologyDrivenViolenceAgainstWomen (Last accessed: 16 November, 2018).

Bytes for All, Pakistan, "Loss of privacy is always permanent - Snags in hearing of FinFisher case at Lahore High Court", (2014). http://content.bytesforall.pk/node/143. (Last accessed: 16 November, 2018).

Bytes for All, Pakistan, "RTI Requests - National Database and Registration Authority (NADRA)", (2016). http://rtirequests.pk/subject-of-rti-request-national-database-and-registration-authority-nadra/ (Last accessed: 16 November, 2018).

Cannataci, Joe. OHCHR, Report of the SR on the right to privacy, A/HRC/34/60. 34th session of the UN Human Rights Council. www.ohchr.org/EN/HRBodies/HRC/RegularSessions/.../A_HRC_34_60_EN.docx

Collin, B. *The future of cyber terrorism*, Proceedings of 11th Annual International Symposium on Criminal Justice Issues, The University of Illinois at Chicago, Denning.

Council of Europe Data protection, human rights and democratic values, XIII Conference of the Data Commissioners 2-4 October 1991.

Council of Europe Report of Commissioner for Human Rights, *The rule of law on the Internet and in the wider digital world*, December, (2014).

D. Kaye, Report on Protection of Sources and Whistleblowers, (2015).

Dahan, Michael. "Hacking for the homeland: Patriotic hackers versus hacktivists." In *ICIW 2013 Proceedings of the 8th International Conference on Information Warfare and Security: ICIW 2013*, p. 51. Academic Conferences Limited, 2013.

David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32, (2015).

Developments in the Field of Information and Telecommunications in the Context of

European Parliament, Scientific and Technological Options Assessment (STOA), An Appraisal of Technologies of Political Control, 6 January, (1998), Online available at: http://jya.com/stoa-atpc.htm (Last accessed: 20 November, 2018).

Executive Office of the President of the United States, "Big Data: Seizing Opportunities, Preserving Values", May 2014 (Online available and retrieved from: www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf), 2014.

FAD FY 12 CCP Funding of Partners, National Security Agency slide reproduced in Glenn Greenwald, No Place to Hide, p. 124. http://glenngreenwald.net/pdf/NoPlaceToHide-Documents-Compressed.pdf (Last accessed: 16 November, 2018).

Final Report of the Roadmap Task, D2.6/Issue 1.1. 2003. Online available at: http://ftp.cwi.nl/CWIreports/PNA/PNA-E0303.pdf, (Last accessed: 20 November, 2018).

Freedom on the Net 2016, Country Profile: Pakistan, Freedom on the Net 2016 , Freedom House, 14 Nov. 2016, www.freedomhouse.org/report/freedom-net/2016/pakistan (Last accessed: 16 November, 2018).

Gercke, Marco. *Understanding Cyber crime: Phenomena, Challenges and Legal Response.* Geneva: International Telecommunication Unit. 2012.

Global Risks Report 2015. 10th Edition is published by the World Economic Forum within the framework of The Global Competitiveness and Benchmarking Network.

Godse, V. "Building an Ecosystem for Cyber Security and Data Protection in India", In: Kumar A., Zhang D. (eds) Ethics and Policy of Biometrics. ICEB 2010. Lecture Notes in Computer Science, vol 6005. Springer, Berlin, Heidelberg. 2010.

Haroon Baloch, "Internet Rights and Legislation in Pakistan: A Critique on Cyber Crime Bill 2016", http://www. netfreedom. pk/ wp- content/ uploads/2016/06/CSO- criticism- on-PECB-2016_IssuePaper (Last accessed: 16 November, 2018).

Hert, Paul de & Schreuders, Eric. "The Relevance of Convention 108", Paper presented at the European Conference on Data Protection on Council of Europe Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data: Present and Future in Warsaw, Poland 34 (2001).

HM Government. "The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world". November 2011.

House of Lords, Science and Technology Committee, Fifth report, "Digital images as evidence". 3 February, 1998.

Human Rights Council, report of special rapporteurs on the right to privacy, 26 February to 23 March 2018

Independent, "Pakistan blasphemy laws increasingly misused to settle petty disputes against Christians", (2012). https://www.independent.co.uk/ news/world/asia/pakistan-blasphemy-

laws-increasingly-misused-to-settle-petty-disputes-against-christians-a6768546.html (Last accessed: 16 November, 2018).

Institute for Economics & Peace. Global Terrorism Index 2020: Measuring the Impact of Terrorism, Sydney, November 2020. Available from: http://visionofhumanity.org/reports (Last accessed: 30 March, 2021).

ITU, A Comparative Analysis of Cybersecurity Initiatives Worldwide, in WSIS Thematic Meeting on Cybersecurity. 2005.

J Lanchester, "The Snowden files: Why the British public should be worried about GCHQ", The Guardian 3 October, (2014).

J. A. Shah, "Report of the Group of Experts on Privacy," 12 Oct, (2012).

Jamil, Zahid. "Cyber Law, Presented at the 50th anniversary celebrations of the Supreme Court of Pakistan". International Judicial Conference on 11-14 August, (2006), Jamil and Jamil Law Associates, Islamabad.

Joint Statement from Article 19, Human Rights Watch, Privacy International, Digital Rights Foundation, and others on the Prevention of Electronic Crimes Bill 2015 Pakistan, online available at: www.privacyinternational.org/sites/default/files/Prevention-of-Electronic-Crimes-Bill-International-Joint-Statement_2.pdf (Last accessed: 20 November, 2018).

Junior, Moneeb. "Cyber Secure Pakistan 2018", International Cyber Security Conference held in Islamabad, 29 Mar, (2018).

Khilji, Usama & Zahid, Saleha. The Internet Policymaking Landscape in Pakistan, An Internet Policy Observatory Publication, Annenberg School for Communication, University of

Pennsylvania, 3620 Walnut St., Philadelphia, Online available at: www.asc.upenn.edu, 215-898-7041 p13 (Last accessed: 20 November, 2018).

Kirby, Michael. The History, Achievement, and Future of the 1980 OECD Guidelines on Privacy, Address at the Round Table on the 30th Anniversary of the OECD Guidelines on Privacy in Paris, France (10 March, 2010).

KPMG Report. Global eFraud Survey, KPMG Forensic and Litigation Services. 2013.

KPMG. *Global eFraud Survey*. KPMG Forensic and Litigation Services. 2013.

M. B. Malik, "Pakistan & India Cyber Secuirty Strategy," 2 June, (2016).

M. P. Omtzigt, "Committee on Legal Affairs and Human Rights," 26 Jan, (2015).

M. Rice, "Tipping the scales: Security & surveillance in Pakistan". (2015). https://www.privacyinter-national.org/sites/default/files/Pakistan%20report%20high%20res%20150723_0.pd (Last accessed: 16 November, 2018).

New South Wales Independent Commission against Corruption, Weighing the waste: An investigation into the conduct at local council waste depot weighbridges at St Peters and Elsewhere, New South Wales Independent Commission against Corruption, Sydney 1999.

Note, Secret Surveillance and the European Convention on Human Rights, 33 *Stanford Law Review*, 1113, 1122. 1981.

Official Records of the General Assembly, Forty-third Session, Supplement No. 40 (A/43/40), annex VI, para. 8.

OIC-CERT Annual Report 2016, 31 Dec, (2016).

Online: Encryption, online anonymity, and human rights. http://hrp.law. harvard.edu/wp-content/uploads/2015/06/Securing-Safe-Spaces-Online-2.pdf (Last accessed: 16 November, 2018).

Organisation for Economic Co-operation and Development, Working Party on Information Security and Privacy, Biometric-Based Technologies, Organisation for Economic Cooperation and Development, Paris. 2004.

Pakistan Assessment 2011, Online available at: http://www.satp.org/satporgtp/countries/pakistan/. (Last accessed: 16 November, 2018).

Pakistan Assessment Report (2011), Online available and retrieved from: http://www.satp.org/satporgtp/countries/pakistan/. (Last accessed: 20 November, 2018).

Pakistan Telecommunications Authority (PTA), "Cellular Mobile", 28 March, (2014), http://www.pta.gov.pk/index.php?Itemid=135 (Last accessed: 16 November, 2018).

Pakistan World Press Freedom Index 2017, "Reporters Without Borders", https://rsf.org/en/pakistan (Last accessed: 16 November, 2018)

Pakistani SIM users given until 17 May to register, Telegeography, 27 April, (2011), https://www.telegeography.com/products/commsupdate/articles/2011/04/27/pakistani-sim-users-given-until-17-may-to-register/ (Last accessed: 16 November, 2018).

PakWired, "How Secure Are NADRA's Critical Information Systems?", (2016). https://pakwired.com/how-secure-are-nadras-critical-information-systems/ (Last accessed: 16 November, 2018).

Privacy Commissioner, 1999-2000 Annual Report, May 2000, Online available and

Privacy International, "State of Privacy Pakistan," 01 Jan, (2018). Online available and retrieved from: https://privacyinternational.org/state-privacy/1008/state-privacy-pakistan (Last accessed: 16 November, 2018).

Privacy International, July 21, 2015, https://www.privacyinternational.org/sites/default/files/2018-02/Privacy-International-Legal-Briefing-10- Human.pdf

Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Committee on Deterring Cyberattacks: Informing Strategies and Developing Options; National Research Council. 2010.

Prof. Joseph Cannataci, the first special rapporteur on the right to privacy https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=22762&LangID=E (Last accessed: 26 September, 2020)

PTA blocks Freedom on the Net Report, https://propakistani.pk/2017/11/17/pta-blocks-freedom-net-report-pakistan/ (Last accessed: 16 November, 2018).

Rahman, Taimur. "The Internet, Youth and Education in Pakistan". National Human Development Report 2015. 2015.

Report of the Senate Committee on Defence and Defence Production http://senate.gov.pk/uploads/documents/1378101374_113.pdf

Report "Pakistan Law," Government Of Pakistan, 31 Dec, (2007).

Report by A. Ananthalakshmi in Kuala Lumpur and Tom Bergin in London; Editing by Raju Gopalakrishnan and Nick Zieminski, "Malaysian central bank says foiled attempted cyberheist", 29 March, (2018).

Report by Eduard Kovacs. Internet and enterprise security news, *insight and analysis.* 2016.

Report of "Pakistan Information Security Association," Online available: https://www.pisa.org.pk/. (Last accessed: 16 November, 2018).

Report of Bytes for All Pakistan, "Pakistan's Internet Landscape", November (2013), http://content.bytesforall.pk/sites/default/files/MappingReportFinal%20-%20Published.pdf

Report of Digital Rights Foundation, "Surveillance of Female Journalists in Pakistan", (2016).

Report of European Commission Joint Research Centre, Institute for Prospective Technology Studies. 2005.

Report of Federal Trade Commission titled: "Protecting Children's Privacy under COPPA: A survey of Compliance", 2 April. (2002).

Report of Freedom House, "Freedom on the Net 2017," 01 Jan, (2017).

Report of HRW. "Privacy and Human Rights. Overview", (2003).

Report of Ministry of Strategy and Finance. "2011 Modularization of Korea's Development Experience: Information Security Activities in Korea". 2012.

Report of National Database and Registration Authority (NADRA), "Solutions", (2015), https://www.nadra.gov.pk/index.php/solutions (Last accessed: 16 November, 2018).

Report of Privacy International (2015), Tipping the Scales: surveillance and security in Pakistan. Available: https://www.privacyinternational.org/sites/default/files/PAKISTAN%20REPORT%20HIGH%20RES%20201507231_0.pdf (Last accessed: 16 November, 2018).

Report of Privacy International, "State of Privacy Pakistan," 01 Jan, (2018).

Report of ProPakistani, "NADRA Has Issued 101 Million ID Cards, Blocked 125K Fake Cards, (2016). https://propakistani.pk/2015/11/26/nadra-has-issued-101-million-id-cards-blocked-125k-fake-cards/ (Last accessed: 16 November, 2018).

Report of ProPakistani, NADRA Shuts Down Its Whistleblower Program, (2016). https://propakistani.pk/2016/04/13/nadra-shuts-down-its-whistleblower-programme/ (Last accessed: 16 November, 2018).

Report of the office of Technology Assessment, New Technology, New Tensions, September. 1987.

Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, Human rights Council Resolution: [illegible].

Report of the Second BITE Scientific Meeting, Tuesday 26th April 2005, Rome, Italy, Biometric Information Technology Ethics (2005). Biometrics and Privacy. Online available online at: http://www.biteproject.org/documents/report_biometrics_privacy.pdf, (Last accessed: 20 November, 2018).

Report of the Senate Committee on Defence and Defence Production, Senate of Pakistan, August-September, (2013), http://www.senate.gov.pk/uploads/documents/1378101374_113.pdf (Last accessed: 16 November, 2018

Report of the UN OHCHR, Online available and retrieved from: http://tbinternet.ohchr.org/_layouts/TreatyBodyExternal/Treaty.aspx?CountryID=131&Lang=EN (Last accessed: 16 November, 2018).

Report of the UN Special Rapporteur on Freedom of Expression, Report (17 April, 2013), UN Doc. A/HRC/23/40, p81.

Report on Electronic Monitoring & Surveillance, American Management Association. 1997. Online available at: <http://www.amanet.org/survey/elec97.htm> (Last accessed: 20 November, 2018).

Report titled: "Cyberspace Policy Review-Assuring a Trusted and Resilient Information and Communications Infrastructure". 2009.

Report titled: "Human Rights in Arab Countries: Bridging the Gulf", online available and retrieved from: http://www.bridgingthegulf.org/links/human-rights-ngos.html (Last accessed: 20 November, 2018)

retrieved from: http://www.privcom.gc.ca/english/02_04_08_e.htm. (Last accessed: 16 Nov, 2018).

Ryssdal, Rolv. Data Protection and the European Convention on Human Rights in

S. A. Ahsan, "Current situation and Issues of Illegal and harmful activities in the field of Information and Communication Technology in Pakistan," 01 Nov, (2002).

Salman Haider, "Front Line Defenders", (2017). https://www.frontlinedefenders.org/en/profile/salman-haider (Last accessed: 16 November, 2018).

Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World

Samar Abbas, "Front Line Defenders", (2017). https://www.frontlinedefenders.org/en/profile/samar-abbas (Last accessed: 16 November, 2018).

Senate of Pakistan, "Report of the Senate Committee on Defence and Defence Production," 01 Sep, (2013).

Special rapporteur on the right to privacy presents first report https://ijrcenter.org/2016/03/30/special-rapporteur-on-the-right-to-privacy-presents-first-report/ (Last accessed: 26 September, 2020))

Special rapporteur on the right to privacy presents first report https://ijrcenter.org/2016/03/30/special-rapporteur-on-the-right-to-privacy-presents-first-report/ (Last accessed: 26 September, 2020))

Surveillance of Female Journalists in Pakistan, Digital Rights Foundation, 31 December, (2016).

T. Ahmed, "Pakistan: National Assembly Passes New Cybercrime Law," 21 Sep, (2016).

The South Asian Association of Regional Cooperation (SAARC) https://www.saarc-sec.org/index.php/about-saarc/about-saarc (Last assessed: 27 September, 2020)

The UNODC Commission on Crime Prevention and Criminal Justice to establish, an open-ended intergovernmental expert group.

The White House. "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure". 2009.

UN special rapporteur on the right to privacy calls on countries to accede to convention 108+ coe.int/en/web/data-protection/-/un-special-rapporteur-on-the-right-to-privacy-calls-on-countries-to-accede-to-convention-108- (Last accessed: 26 September, 2020)

Resolutions and Guidelines

A/RES/*55/63*.

A/RES/*56/121*.

A/RES/*57/239*.

A/RES/58/199.

A/RES/65/230.

A/RES/67/189.

Eritrea/Yemen Arbitration (Phase One: Territorial Sovereignty and Scope of Dispute) 9 October 1999.

International Security, 4 January 1999, A/RES/53/70.

ITU, A Comparative Analysis of Cybersecurity Initiatives Worldwide, in WSIS Thematic Meeting on Cybersecurity. 2005: Geneva

O.A.S. Res XXX, adopted by the Ninth Conference of American States, 1948 OEA/Ser/. L./V/I.4 Rev (1965).

Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children Special measures to be adopted to fight the menace of international terrorism, resolution adopted by the General Assembly, on its 2nd meeting, held on 23 March 2010, A/RES/4/3.

The UN Guidelines Concerning Computerized Personal Data Files, G.A. Res. 45/90, U.N. Doc. A/RES/45/90 (1990).

The United Nations Global Counter-Terrorism Strategy, 20 September 2006 A/RES/60/288.

The United Nations, Resolution adopted by the General Assembly on 18 December 2014, 69/166. The right to privacy in the digital age, A/RES/69/166, 10 February, (2015), online at: www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/166 (Last accessed: 16 November, 2018)

UN General Assembly Resolution, The Right to Privacy in the Digital Age, UN Doc 68/167 (14 December 2013).

UN General Assembly Resolution, The Right to Privacy in the Digital Age, UN Doc 66/169 (14 December 2014).

UN General Assembly Resolution, The Right to Privacy in the Digital Age, UN Doc A.3/71/L.39/Rev.1 (16 November 2016).

UN General Assembly, 'Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms' Adopted by General Assembly Resolution 53/144 (9 December 1998).

UN General Assembly, 'Report of Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' UN Doc A/68/98 (24 June 2013).

UN General Assembly, 'Special Report of the Disarmament Commission to the General Assembly at its Third Special Session Devoted to Disarmament' (28 May 2006) UN Doc A/S-15/3.

UN General Assembly, Resolution 60/251 (2006) UN Doc A/Res/251.

UNGA Doc A/RES/44/25 (12 December 1989) with Annex, Article 16.

UNGA Resolution 68/167: The right to privacy in the digital age, 18 December 2013, online at: www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167 (Last accessed: 16 November, 2018).

United States Declaration of Independence, (1776).

Webliography

csrc.nist.gov (Last accessed: 20 November, 2018)

http://cyberbullying.us/ (Last accessed: 20 November, 2018)

http://cyberlaw.stanford.edu/our-work/cases (Last accessed: 20 November, 2018)

http://cyberlawcases.com/ (Last accessed: 20 November, 2018)

http://investinpakistan.pk/pdf/National_IT_Policy.pdf. (Last accessed: 20 November, 2018)

http://partners.nytimes.com/library/tech/reference/indexcyberlaw.html (Last accessed: 20 November, 2018)

http://pklegal.org/content/legal-services-relating-cyber-crimes-laws-pakistan (Last accessed: 20 November, 2018)

http://tribune.com.pk/story/718865/cyber-crime-fia-arrests-alleged-facebook-blackmailer (Last accessed: 20 November, 2018)

http://uscode.house.gov/ (Last accessed: 20 November, 2018)

http://www.coe.int (Last accessed: 20 November, 2018)

http://www.cybercrimelaw.net (Last accessed: 20 November, 2018)

http://www.cybercrimelaw.net/Cybercrimelaw.html (Last accessed: 20 November, 2018)

http://www.cyberlawclinic.org/casestudy.asp (Last accessed: 20 November, 2018)

http://www.cyberlawdb.com/gcld/ (Last accessed: 20 November, 2018)

http://www.cyberlawsindia.net/cases.html (Last accessed: 20 November, 2018)

http://www.emeraldinsight.com/doi/abs/10.1108/13639510610684674 (Last accessed: 20 November, 2018)

http://www.justice.gov/criminal/cybercrime/ (Last accessed: 20 November, 2018)

http://www.ljcp.gov.pk/ (Last accessed: 20 November, 2018)

http://www.olemiss.edu/depts/ncjrl/ (Last accessed: 20 November, 2018)

http://www.prashantmali.com/cyber-law-cases (Last accessed: 20 November, 2018)

ITU-D: E-Strategies Unit website, www.itu.int/ITU-D/e-strategy/ (Last accessed: 20 November, 2018)

www.coppa.org (Last accessed: 20 November, 2018)

www.copyright.gov (Last accessed: 20 November, 2018)

www.crs.gov (Last accessed: 20 November, 2018)

www.cybercrime.gov (Last accessed: 20 November, 2018)

www.cyber-rights.org (Last accessed: 20 November, 2018)

www.dawn.com (Last accessed: 20 November, 2018)

www.elibraryusa.gov (Last accessed: 20 November, 2018)

www.gao.gov (Last accessed: 20 November, 2018)

www.govtrack.us (Last accessed: 20 November, 2018)

www.itu.int (Last accessed: 20 November, 2018)

www.oas.org (Last accessed: 20 November, 2018)

www.supremecourt.gov.pk/ijc/articles/10/5.pdf (Last accessed: 20 November, 2018)

www.unodc.org (Last accessed: 20 November, 2018)

www.ussc.gov (Last accessed: 20 November, 2018)

The End