"DATA PROTECTION IN INDIA : A COMPARITIVE STUDY"

A Thesis Submitted To

Nirma University

In Partial Fulfillment Of The Requirements For

The Degree Of

Doctor Of Philosophy

In

Law

BY

SHIVANI JOSHI (11EXTPHDLO2),

Institute Of Law

Nirma University

Ahmedabad – 382481

Gujarat, India.

(August 2019)

Nirma University
Institute of Law
Certificate

This is to certify that the thesis entitled "DATA PROTECTION IN INDIA : A COMPARITIVE STUDY" has been prepared by SHIVANI BHARATBHAI JOSHI under my supervision and guidance. The thesis is her own original work completed after careful research and investigation. The work of the thesis is of the standard expected of a candidate for Ph.D. Programme in Law and I recommend that it be sent for evaluation.

Date: 26/8/19

Signature of the Guide

Forwarded Through:

Prof Dr. Madhuri Patel

(i) Name and signature of the
Head of the Department (if any)

ii) Name and signature of the Dean Faculty of Law

28-8-19

(iii) Name and signature of the Dean Faculty of Doctoral Studies and Research

To:
Executive Registrar
Nirma University

28/8/19

Nirma University
Institute of Law
Declaration

I, SHIVANI JOSHI, registered as Research Scholar, bearing Registration No. EXT11PHDL02 for Doctoral Programme under the Faculty of LAW of Nirma University do hereby declare that I have completed the course work, pre-synopsis seminar and my research work as prescribed under R. Ph.D. 3.5.

I do hereby declare that the thesis submitted is original and is the outcome of the independent investigations / research carried out by me and contains no plagiarism. The research is leading to the discovery of new facts already known. This work has not been submitted to any other University or Body in quest of a degree, diploma or any other kind of academic award.

I do hereby further declare that the text, diagrams or any other material taken from other sources (including but not limited to books, journals and web) have been acknowledged, referred and cited to the best of my knowledge and understanding.

Date: 26/8/19

Signature of the Student.

Signature of the Guide

ABSTRACT

Data Protection was never an issue in India due to its "VASUDEV KUTUMBKUM" culture. For an example, while it is a common practice in the UK for general practitioners (GPs) to not discuss patient information relating to the wife with her husband, such discussion is quite common in India, where GPs regularly discuss such issues not only with the husband but also other members of the family or the person accompanying the patient. When Indian people are questioned about the word "privacy", the first thing that comes to their mind is privacy in terms of personal space and subjects, while the US citizens mentions privacy with reference to financial information and identity theft and that is what the correct and accurate anvil on which privacy must be weighed, protected and tested. With the invincible and unconventional development in technology the issues and concerns around data protection has increased on multiple levels and has surfaced to be a point of discourse in India as well. The scope of 'data' was primitively limited to an individual's mere name, address of communication and that was when data mining was considered an important source of business for consultancy firms and BPOs in India. Earlier data protection concerns was limited to BPOs only, but now, data is collected, altered, indexed, stored, processed, shared, and utilized at various fields in India which has been discussed in the paper. For a dearth of a specialized and an all-inclusive data protection law in India, huge issues and instances of data theft has risen, whether it is on a BPO platform or hunting down of an entire digitalized market of a financial institution, along with several other business sector. So to say, the underlying hypothesis of the paper being that a laid out IT Act, 2000 and rules thereto may prove to be of insufficient role and incomplete to address the rising concerns for individuals as well as organizations, be it boutique or of enterprise level. Banks has to move on national television to advertise about not sharing OTP with any caller pretending to be calling from bank is the extreme condition raised due to lack of stringent codified law for Data Protection. Now the government is raising such situations

for which Aadhaar enrolment becomes mandatory. Such situation can lead to a disastrous result if the Aadhaar details of the citizen is leaked and misused. The prevailing law is not sufficient enough to protection the vast data. Hence, a separate, stringent and codified law is necessary for India.

Contents

Chapter one deals with the introduction to the research work done, research aims and objectives along with research methodology and the structure of the thesis. And lastly the outcome of research is also outlined given in this chapter.

Chapter two shows the historical background of the data protection i.e., how data protection started marking its existence in the world. The evolution of data protection legislation in European Countries, USA and India is discussed at length in this chapter.

Chapter three focuses on Regulatory Provisions related to data protection in the countries like European Union and USA. What are provisions of the data protection legislation followed by these countries are discussed in detail under this chapter.

Chapter four enlightens the Regulatory Framework of the data protection in India i.e., presently how data protection is dealt with in India.

Chapter five compares the Legal Framework related to data protection of India with the Legal Frameworks related to Data Protection of European Union and USA. The detailed analysis of the data collected by the researcher through empirical research is also discussed in this chapter.

The research work ends with Chapter six which is conclusion and recommendations for the data protection into Indian Context along with a suggested draft bill of Data Protection Legislation inspired by the comparison made in chapter 5 of the thesis as the final outcome of the research

ACKNOWLEDGEMENT

This thesis has been very fruitful endeavour, given the contemporary nature of the subject discussed and also its increasing relevance in times to come. I would like to extend my gratitude to several people, who have guided and supported me at each and every stage of this project.

I am very thankful to Nirma University for providing me with the platform for carrying my research work.

I am deeply indebted to my guide Prof. (Dr.) Purvi Pokhariyal, whose constant supervision and motivation has brought out the best in me, which reflects in the findings of my study.

I am extremely thankful to the R.P.C committee member Prof. (Dr.) Purvi Pokhariyal, Dr. S. P. Rathore and Dr. M. I. Baig, for their stimulation suggestions at all the meetings. Without their constant encouragement and guidance, this project would not have seen the light of the day.

I extend my gratitude to the Ph.D Section for the help they had provided whenever I needed for it.

In addition, I would like to extend my gratitude to the two important persons – my mother Mrs. Mangla Joshi and my husband Mr. Jigar Mehta who stood by my side like rocks at all the time and whose enthusiasm, care, concern and energy kept me going all through.

I would like to extend my thanks to Mr. Faiyaz Shaikh who had been very supportive, helpful and encouraging all the time.

Last but not the least my thanks to my wonderful kids Anay and Manay, Mr. Bharat Joshi and Mr. Hiren Patel who has been my biggest strength and support system in my entire endeavour and for making me that person that I am.

Date: August 2019

Shivani B. Joshi

Contents

ABRREVIATIONS

EU Data Protection Directive -- EU DPD

Organization of Economic Co-Operation and Development -- OECD

Freedom of Information Act -- FOIA

People's Union for Civil Liberties -- PUCL

Human Immunodeficiency Virus -- HIV

Information Technology -- IT

EU Data Protection Directive -- EU DPD

Federal Trade Commission Act -- FTCA

Controlling the Assault of Non-solicited Pronography And

Marketing Act. -- CAN-SPAM Act

Payment Card Industry Data Security Standard -- PCI DSS

Aisa-Pacific Economic Co-operation -- APEC

United Nations -- UN

Universal Declaration of Human Rights -- UDHR

Family Educational Rights and Privacy Act -- FERPA

Children's Online Privacy Protection Act -- COPPA

Health Insurance Portability and Accountability Act -- HIPAA

Health Information Technology for Economic and Clinical Health Act -- HITECH

Fair Credit Reporting Act -- FCRA

Gramm-Leach-Bliley Act -- GLBA

internet service providers -- ISP

California Financial Information Privacy Act -- CFPIA

California Online Privacy Protection Act -- Cal. COPPA

California Attorney General -- CA AG

Payment Card Industry Data Security Standard -- PCI DSS

Cross-Border Privacy Rules System -- CBPR System

Treaty on European Union -- TEU

Treaty on the Functioning of the European Union -- TFEU

European Convention on Human Rights -- ECHR

European Court of Human Rights -- ECtHR

Deoxyribonucleic acid -- DNA

European Privacy Seal -- EuroPriSe

Trans-European Telecommunications Networks --TEN

European Network and Information Security Agency -- ENISA

Court Of Justice Of European Union -- CJEU

European Data Protection Supervisor -- EDPS

European Economic Area -- EEA

Passenger Name Records -- PNR

Department of Homeland Security -- DHS

Society for Worldwide Interbank Financial Telecommunication -- SWIFT

Single Euro Payments Area -- SEPA

European Securities and Markets Authority -- ESMA

Individualism Index -- IDV

Power Distance Index -- PDI

United Kingdom -- UK

general practitioners -- GPs

All India Records -- AIR

Supreme Court Cases -- SCC

United Nations Commission on International Trade Law -- UNCITRAL

Information Tecnology Amendment Act -- ITAA

Closed Circuit Television -- CCTV

United States of America -- U.S.A

Business Process Outsourcing -- BPO

European Union -- EU

Information Technology -- IT

Television -- TV

Short Message Service -- SMS

Reserve Bank Of India -- RBI

The Housing Development Finance Corporation -- HDFC

State Bank Of India -- SBI

Personal Identification Number -- PIN

Information Technology Enabled Services-Business Process Outsourcing -- ITES-BPO

DO NOT DISTURB -- DND

Bharat Sanchar Nigam Limited -- BSNL

Subscriber Identity Module -- SIM

Life Insurance Corporation Of India -- LIC

Unique Identification Authority of India -- UIDAI

Social Security Number -- SSN

Public Interest Litigation -- PIL

Right To Information -- RTI

Data Security Council of India -- DSCI

Non-Governmental Organisations -- NGO

European Union -- EU

United States -- US

The National Intelligence Grid -- NATGRID

Crime and Criminal Tracking Network and Systems -- CCTNS

Deoxyribonucleic Acid -- DNA

Information and Communications Technology -- ICT

Foreign Direct Investment -- FDI

CHAPTER 1

INTRODUCTION TO THE RESEARCH

Table Of Contents

1. INTRODUCTION

Information for knowledge based industry is like blood to the life of living beings. Information is worthy supplies not only for businesses like service and manufacturing, but adscititiously it is perilous for economy and security of a nation. The utilization of data/information and its capability to get converted into progressive information is very paramount for businessmen, policymakers, scientists, engineers, etc. Having worthwhile and at times exclusive information can have betterment in productivity and quality which can advance the field of education, research and it supplemental benefits to make denizens more erudite.

Indian culture's point of difference from the Western culture begins with the non-distinctive concept of the autonomous individual. The Western world conceives an individual with the incredible idea, imagining him living within an inviolate protected region, having the liberty "to choose".[1] The holistic Indian culture embraces the very socio-centric belief of collectivism, where the privacy of an individual loses its supremacy, whereas the West encourages the very notion of individualism. India is a collectivist society where individualism or privacy is given less consequentiality as compared to the UK or the US, where an individual's paramountcy is at least equipollent to, if not more preponderant than the importance of the collectivity.[2] This further leads to a varied understanding of the data protection in the minds of individuals hailing from these two cultures. When one from the West will take it to be an issue concerning his privacy, which is paramount to him, an Indian would not only be concerned about his own privacy, but also the societal value combined with his privacy.

Data protection is indistinctively associated with "privacy". With the technological advancements and economic reforms, there is now an extensive demand for protection against incongruous accumulation and handling of data.

[1] Richard A. Shweder & Edmund J. Bourne, *Does the Concept of the Person Vary Cross-Culturally? Abstract visited at website on July 12th 2016*
[2] Hofstede's Book on Cultural Dimensions

There has also been a remarkable intensification of the internet users, consuming the net for information, communication and e-commerce, accentuating on the authoritative ordinance of an efficacious regulatory system, shedding a new light on the accumulation, processing and handling of the data.

The information acquired by the websites may be relegated as either "individually identifiable information", or as "mass undisclosed information". To elaborate on each of these aforementioned terms, one may say that the :

"individually identifiable information" entails authentic information, which has more to do with the identification of an individual. It may incorporate data such as names, addresses, telephone number, credit card number, or email id and other person-specific information. This information may also be linked to the identifiable information of other sources, from which the other related personal information can be extracted with ease. The IP address may also be associated with this information. Other example could be, Processor Serial Number or PSN is a Pentium III processor identifier chip, which is a number fixed to the individual's laptop or desktop or computer and is used to approve one's identity through a scope of communications with any association or statistic.[3] The internet also fosters a trail of data every time a person makes a cessation which may or may not be related to certain personal information.

On the other hand, "Mass undisclosed information" is aggregated or categorized by a website or a third party according to the geographical areas (information such as postal codes and non-consumer concrete information engendered from innominate transactions), to help merchants manage their business and advertising better. [4]

Regardless, a number of technologies are used to accumulate both classes of information on consumers. "Cookies" can be one such example, which saves information in the form of computer code on a user's browser automatically. Cookies are information of the user's personal predilections

[3] Data Safety and Privacy Protection, by Venkararmana B. Ramanathan, available at http://www.legalserviceindia.com/articles/Data_Safety.htm
[4] Data Protection, by R K Dewan available at http://www.rkdewan.com/dataprotection.php

exhibited during their visit to a website[5]. As it is infeasible to differentiate between visitors to a website, the server will somehow mark the visitor by storing information on them.

Introduction of internet had made data transfer much facile which was time consuming earlier. The entire world can be accessed now on a small laptop screens through internet. Every person's life is profoundly affected by this internet. Internet has expunged the territorial barriers to an extent which till now was major impediment for the progress of trans-border business. Along with giving simplified answers to many critical questions, the World Wide Web has major side effect in terms of involuntary disclosure of data. This can be analyzed from these illustrations below:

1. With each sign-in to the electronic mail in the cyber cafes, the electronic trace of password remains there unsecured.[6] This can be misused by others without the cognizance of that individual.

2. With each use of credit card for shopping, the trail of brand predilection, place of shopping etc. are left. Such information can be used for marketing approach.

3. On each sign-in to internet, there is left abaft an electronic trace enabling website owners and advertising companies to get access to the predilection and culls of the users by tracking them.

4. Unwanted e-mails are withal a customary practice of accumulating personal information of the users.

5. Places for shopping collects personal data for promotions and exchanges such data with advertisers without the consent of the data subject.

With the absence of a stringent law relating to data protection, the miscreants are encouraged to become adroit in their mischief with each passing day.

5 Data Protection Overview by - Tapan Ray.
[6] Data Protection In India, by Pankaj Kumar available at http://www.legalserviceindia.com/article/l37-Data-Protection-Law-in-India.html

Considering the same, one can easily see how an innocent user provides room for the internet frauds to develop and simplify their acts. Maintaining the integrity of the data is an arduous task, especially with the continuous technological development, the methods of crimes keep evolving. Today, cyber-crime has become a pest, as the prurience of information acts as a catalyst in growth of the same.

Maintaining integrity of data is much arduous task. With incipient technological development an evolution took place in the method of crimes. Today criminal like professionals carry out their crimes through the medium like computers and electronic contrivances. The abundance of information is acting as a promoter in the growth of cyber-crimes. The highest quandary faced by the business houses, financial institutions and the governmental bodies now a days is, how to provide adequate protection to their immensely colossal data. In the absence of any stringent law relating to data protection, the miscreants are becoming adroit in their work day by day.

2. ***PANORAMIC VIEW OF THE THESIS***

Information is one of the most valued and at the same time controversial element of modern life. Both governmental and private bodies have prodigious amount of information about individuals, however, the regulation with reference to, who has this information, how they can hold it, and in what circumstances they use it or pass it on to others, has been the subject of detailed legislation and guidance over many years. Albeit data have always been valued, their worthiness was not as greatly esteemed as it is today. With the development in technologies there arose desideratum of trade secret, misappropriation and inequitable competition laws, contracts, and technological protection measures. In last few decades, those who accumulated or have an access to sizably voluminous amount of data has commenced to find ways to utilise the collected data as their source of income. The development of legislations for the protection of data assets has become more captivating at the international grounds, because of the data flow from one

country to another. Countries providing strong data protection inclined investment towards them from data providers. However, countries providing weaker protection equally attracted businesses but if, protection is minimal, these countries were heavenly for data pirates.

Conceptually, data protection can be explicated as :- "Giving felicitous reverence and treatment to the information cognate to an individual". Data protection focuses on issues relating to the collection, storage, accuracy and use of data provided by the data subject. Net users using the World Wide Web want their privacy rights to be venerated when they engage in e-Commerce. It is component of the confidence-creating role that successful e-Commerce businesses have to convey to the consumer. If industry doesn't ascertain it's guarding the privacy of the data it accumulates, it will be the responsibility of the government and it's their obligation to enact legislation. The quandary that arises in Electronic Commerce is, that the Internet itself global. The protection of personal data was never a national problem rather it was always a global issue.[7]

India has come up as the host of data outsourcing and processing and therefore India can be considered as the main point of data theft as there is absence of specific law relating to data protection. The economic industry of India handles and accesses all types of data (personal as well as non-personal) belonging to the people of the world. Crucial amongst this data is credit card information, financial information and medical information of an individual. The outsourcing companies store such confidential information to which their employees have access and hence the risk of data theft in absence of law is at highest rate. There are cases of security fissures and data leaks in the high profile Indian companies. And such incident raises concerns for data protection in the Indian BPO industry.[8]

Indian companies operate without concrete licit essentialities related to data protection, other than those levied by contract. Depending on the

[7] Data Protection, by R K Dewan available at http://www.rkdewan.com/dataprotection.php
[8] Data Protection Act in India with Compared to Europena Union Countries, by Danish Jamil and Muhammad Numan Ali Khan, published by International Journal of Electrical and Computer Sciences Vol 11 No. 6.

provisions making data protection mandatory under the contract, the level of protections will fluctuate extensively from company to company, and perhaps from client to client. Business corruption perpetuates to be a perceived problem in India, affecting the level of confidence by foreign companies in Indian BPOs. Apperceiving the desideratum to provide assurances of data protection to its foreign clients, many BPO service providers in India have engaged in self- regulation for addressing the unexpected damage that may inflict on the BPO industry resulting from major security abuses.[9]

The last data protection bill, The Personal Data Protection Bill 2006, introduced in Parliament on 8 December 2006, has been lapsed. On 18 October 2010, the Department of Personnel and Training, Government of India, published an approach paper for legislation on privacy. The objective abaft this research was to examine the issues and challenges involved in protecting data. Rajeev Chandrashekhar, an MP came up with The Right To Privacy Bill at Rajya Sabha in February 2011. Protection to the privacy of a person including public figures was the main focus point of the Bill. While analysing the Bill, it seems that the bill focuses on safeguarding the use of electronic/digital recording devices in public spaces without consent rather than focusing on protecting individual's privacy.[10] However, the bill had never passed.

If it was not for this rapidly increasing off-shoring business and the Unique Identification Number program, India would perhaps never have worried much about data protection, as there are already existing provisions in Indian licit framework for protection of data, though not at the scale at which protection is warranted under the current circumstances. The Aadhaar number, which is a single identifier of Indian citizen globally, is supposed to work across application domains which make individuals vulnerable to privacy breaches. In an Aadhaar like setup, the biggest threat to privacy emanates from potential insider leaks. The Aadhaar program does not seem to have been

[9] Attitudes Towards Privacy: A Comparison of India and the United States, by Jane Hils Shea. Visited at website on September 26th 2013.
[10] Right To Privacy Bill 2010 – A Few Comments, by Elonnai Hickok. Visited at website on August 15th 2015.

explicitly designed to have vigorous protections against such insider leaks. It seems that efficacious protection against insider leaks indispensably requires a data controller at UID headquarters as well as at the companies hired for the collection of data on behalf of the government. UID program has commenced and various complaints also have been registered against the company hired for accumulation of data by the government at several places. Thus, though there are earnest privacy concerns at present, we believe that Aadhaar can be made safe from the legal perspective by enacting a legal framework for data protection for concrete paramount reinforcing. Perhaps the single most paramount concrete question that scrounges answering is who should have the right to verify the identity of an individual, and under what circumstances? Though Aadhaar Act has been enacted but a stringent single codified law is needed for the better protection of data in India.

3. ***STATEMENT OF PROBLEM***

There has been a vigorous opinion that if India fortifies its data protection law to attract multi-national corporations to India. India instead of being a mere supplier of services can act as host to such corporations.[11] The discussion regarding the lack of data protection legislation in India heated up when the Indian information technology industry grabbed a major role in the outsourcing business. There has been extensive discussion about how this may impact upon the flow of outsourcing business from European Union countries.[12]

This debate became much crucial after the prelude of Aadhaar Card Program carried by the government of India. The delay in Indian enactment of data protection legislation raised concerns that this might divert outsourcing

[11] What are the laws - Data Protection, Data Transmission and Export and Data Encryption in India to operate a technology platform for data processing? Answer by Prakash Prasad available on https://www.quora.com/What-are-the-laws-Data-Protection-Data-Transmission-and-Export-and-Data-Encryption-in-India-to-operate-a-technology-platform-for-data-processing

[12] India's New Data Protection Legislation, by Raghunath Ananthapur, published in journal named Scripted available at https://script-ed.org/article/indias-data-protection-legislation/

business from the European Union to other countries that provide adequate levels of protection for personal data via legislative designates [13]. India's business, data and knowledge process outsourcing industries have shown remarkable growth in the last few years. However, various incidents of data theft and misuse of private and personal information have raised concerns and doubt about outsourcing to India.[14]

The recent opinion by Supreme Court has made obligatory for production of only PAN card and not Aadhaar Card for filing IT return. Court also ruled out that Aadhaar does not infringe on an individual's right to privacy and upheld its constitutional validity. Several sections of the Act were struck down. Court struck down Section 57 of the Aadhaar Act considering it as "unconstitutional". This implies no organization or private substance can seek for Aadhaar ID from you, this implies no privately owned business can constrain you to present your Aadhaar data to buy or avail their service benefits.

Circular issued by TRAI in March 2017 mandating linking of mobile number with Aadhaar was striked down referring it to be illegal and unconstitutional as it is not supported by any law. As indicated by the judgment given by the apex court, banks and other financial institutions cannot seek Aadhaar data. The top court additionally included that educational organizations alongside UGC, NEET, and CBSE can't take Aadhaar amid for admissions or enrolment which was a fundamental condition before. The judgment mandated parental or guardian's consent before enrolment of children under Aadhar Act. The judgement further provides that children attaining the age of majority has the right to exit from Aadhaar in case they are enrolled under Aadhaar through their parental consent.

Section 33(2) of the Aadhaar Act, which says that it is legal to disclose identity and authenticated data in the interest of national security on direction

13 Report Group of Experts on Privacy by Government of India
[14] Data Protection In India, article by Majmudar & Co. available at https://www.scribd.com/document/136287003/Data-Protection-in-India

of an officer not below the rank of Joint Secretary to the government of India was struck down by the apex court. Section 47 of the Aadhaar Act, which says that no individual was allowed to file a complaint if he/she felt their data was leaked or misused, was also ruled out by the Supreme Court. Under this Section, the law only allowed the court to take cognizance of a complaint filed by UIDAI or anyone authorized by it.

Authentication data record should not be kept beyond six months was made clear in the judgement by the Supreme Court and the provision that allowed archive records for five years has also been struck down. Storage of meta data of transactions by individuals is excluded by the apex court in the judgement. This banning implies that UIDAI cannot collect data sets and mine it for more data or analysis. Data sharing with the corporates is also ruled out. The Supreme Court also called for Parliament to draft and pass a data protection law as early as possible. After effect of judgment has forced UIADI to make provisions for unlinking Aadhar card which was deemed mandatory previously. UIADI has now asked all private entities like banks and telecom companies to submit plan to stop use of Aadhar data.

In 2017 and 2018 status of data protection in India was the focal point of numerous discourses. The presence of privacy as one of the fundamental right was confronted by the government before the Supreme Court. Promoters favoring privacy were viewed as differentiating the estimations of Indian culture. Endeavours for framing a separate legislation for data protection were in vein. The most recent judgment of Supreme Court on Aadhaar confronted the manner personal data is protected in India.

On 24 August 2017, a nine-judge bench of the Supreme Court laid down judgment, together upholding that privacy was a fundamental right, retaining individual's nobility and independence and expressing it as the core of the constitutional order. Privacy in this technologically advanced world is no more an extravagance concern; it influences each person as it is pervasive through the mode of web. By the end of July, Justice B. N. Shrikrishna Committee was appointed by the government who came up with a report along with a draft bill for data protection for India.

Since the government delayed the implementation of a legal framework for prosecution of data and privacy breaches, Indian BPO companies have therefore implemented unified processes such as the BS7799 and the ISO17799 standards for information security management, which also explicitly restrict the quantity of data that is available to employees of BPO and call centres. Indian government needs to implement a strong Data Protection Act to sustain the BPO business and parallely have a secured Aadhaar Card system. Still if the government doesn't act on an effective data protection then a there are chances that India may completely loose BPO business and if data is misused under Aadhaar Scheme than it can lead to a undesirable result and can even cause threat to the nation once huge amount to citizen record is easily accessible without any proper protection.

A data protection authority with a proper framework in place would have helped in curbing the present issues. The Authority would have had all mandates for collecting, processing, archiving and purging aadhar information and the current mess could have been avoided. Apart from this an immensely colossal data has been accumulated by the private agencies for Aadhaar card; this Aadhaar number contains personal details of the citizen of India. Hence, protecting Aadhaar number under a stringent law is much more obligatory to evade any disastrous offence which can bring an citizen under extreme trouble.

4. ***RESEARCH OBJECTIVES AND AIMS***

At the outset of all the developments mentioned above, India needs to enact data protection legislation respecting the protection of personal and non-personal as well as sensitive personal data. Hence, aims and objectives of research are based on above mentioned issues.

The aims and objectives of the research are as follow:

1. To carry out comparison between the laws relating to data protection in the countries like USA and European Union, and the way data is being protected in India.

2. To investigate the standards on which the laws of these nations are based. The further exploration looks at how well the Indian draft Data Protection bill fares in comparison to other global standards.

3. To evaluate and examine the present legal scenario of India for the data protection.

4. To examine the consequences prevailing in India in the absence of a law as well as to examine further over the need to have legislation on Data Protection for India with reference to UID Project.

5. To suggest a Draft Bill for the Data Protection Legislation into Indian Context is the last and vital aim of the research.

5. ***HYPOTHESIS***

1) That the separate codified Data Protection Law is the necessity for India.

2) That the issues related to data theft would not haunt the investor after enactment of a codified Data Protection Law.

3) That the Data Protection Legislation if enacted will give complete protection to the Aadhaar Card scheme.

6. ***RESEARCH QUESTIONS***

In order to examine above mentioned hypothesis, following research questions are required to be answered:

1. What is the present scenario for data protection in India?

2. What are the consequences for India in the absence of explicit data protection law

3. What considerations need to be taken in to account while drafting Data Protection Law for India?

7. RESEARCH METHODOLOGY

The methodology adopted in the study is both doctrinal and empirical.

7.1 Doctrinal Research Methods

Doctrinal study includes analysis of research articles, books, reports, treaties, conventions, statutes, and cases decided by courts. Some of the books referred to carry doctrinal research here were about cultures of different countries. Going through these books helped the researcher to showcase that Indian notions relating to privacy are different from other countries. While other articles referred by the researcher made her understand about the perception of data or privacy protection in the European countries and USA. The others books referred were about Constitution of India, how to carry governance in corporate world by managers for data protection, studying the data protection directives and its implementation by the countries of EU, etc. The web articles referred by the researcher were majorly about the latest update of data protection in India. The other article referred also takes the researcher towards the need for enacting data protection law in India. Several articles made the understanding of complicated laws easy for the researcher. Treaties, conventions and statutes were studied to have a better idea about the law prevailing in different countries and agreement made by different countries for implementing data protection.

Doctrinal research helps the researcher to carry out her comparative study for the law. Moreover focus of the researcher while carrying the comparative study was on functional comparison amongst the various kinds of comparative studies. Functional comparison method is applied along with the teleological method (teleological method is taking into account a given thing's purpose) for serving different goals, understanding law properly, focusing on similarities if any, critical analysis of essentials required for a legislation, determining a better law and unifying law (with any international treaty or agreement), critical appraisal of basic necessities required to draft a particular law, etc. The researcher has applied functional comparison for the purpose of pointing out the importance of research objectives and research questions

which involves law reform and enactment of legislation with separate entity relating to data protection. This above said approach consists of ascertaining the essentials to be taken into consideration for drafting legislation; the cultural differences existed amongst the countries in comparison, and examining their operation in the context of social environment in which legal system operates. The functional comparison approach helped the researcher to analyse legal rules vital for data protection legislation in these modern times for India.

7.2 Non-Doctrinal Research Methods

The study also includes empirical study for which data is collected from the field. During the field study, the tools used for the collection of data are interview and questionnaires. The samples for the study have been drawn by random sampling method. Data for the study is collected from national call centres, international call centres, multispecialty hospitals, small clinics (especially maternity homes), schools, banks, insurance companies, pathology laboratory and common public to get the true picture of the problem. The data collected has been analysed. The standard form of citation and references are used in the study.

For questionnaire method, set of separate questions were prepared for multispecialty hospitals, small clinics (especially maternity homes), schools, banks, insurance companies, pathology laboratory and common public respectively. The questionnaire was drafted using Google Docs and then e-mailed as well as handed over personally as hard copy to the target respondents. The questionnaire send through mail were responded back electronically while questionnaire handed over personally were reverted back in the same manner. Overall the response from all the persons, who were directly or indirectly associated with the survey, was excellent. The responses gathered by researcher were quiet satisfactory and was much useful to lead the research further.

The target respondents amongst common public were from the age of 25 to 65. Approximately 150 questionnaires were distributed amongst common

public across Ahmedabad and Vadodara to have an idea about the how important data protection is considered by them. The researcher has used random sampling method, and the public selected worked in different fields like house wives, business person, teacher, free lancers, employees of advertising companies, lawyers, and so on. The researcher has not confined to one particular class of people for sampling. The subject of the research is such that the researcher had to select educated public so that they can intellectually answer the question addressed in the questionnaire.

The other sample selected by the researcher was HR of multispecialty hospitals at Udaipur and Ahmedabad. Three hospitals of Ahmedabad and two hospitals of Udaipur were selected by the researcher. Here the question of data relating to health is in concern. After carrying the research at the multispecialty hospitals the researcher lastly studied the position at the private maternity clinics of the doctors. Here the sample selected by the researcher was receptionist of private clinics especially maternity clinics across Ahmedabad and Vadodara. The selection method was random sampling method, five maternity clinics from the satellite area of Ahmedabad and two maternity clinics from manjalpur area of Vadodara were approached for the research.

Further the team leader of national call centres at Ahmedabad, Vadodara, Goa and Mumbai as well as manager of the international call centres at Ahmedabad and Mumbai was selected as samples by the researcher to accomplish her research in the field of Business Processing Organizations. Three national call centres from Ahmedabad, two national call centres from Vadodara and one national call centre from Goa were selected by the researcher through random sampling method. Whereas two international call centres from Ahmedabad, one international call centre from Goa and one international call centre from Mumbai was selected by the researcher through random sampling method to carry the research work.

The employees of bank from Vadodara and Ahmedabad were also given with the questionnaire to have the true reality of data protection at banks. Banks possesses the financial data of their customers which is one of the

crucial personal data. Two banks from Vadodara and three banks from Ahmedabad were selected by the researcher through random sampling method to carry the research.

Further the researcher has extended the area of research to educational institutions like pre-schools. Here the sample selected by the researcher was the principal of pre-schools at Ahmedabad and Vadodara. Five pre-schools from each city were selected involving random sampling method. To be more specific five pre-schools from the satellite area of Ahmedabad and five pre-schools from the manjalpur area of Vadodara were selected for carrying the research.

Pathology laboratory collects the blood samples of the patients from which DNA can be extracted and DNA comprises a part of sensitive personal data. Hence, the researcher extended her research area and included pathology laboratory also as it was important for the subject matter of the research. The samples selected by the researcher through random sampling method were the employee of pathology laboratory at the satellite area of Ahmedabad. Five pathology laboratories in the satellite area of Ahmedabad were selected for carrying the research.

The other area of research included by the researcher is the Insurance Companies specifically Life Insurance Company. The sample selected for carrying research in this area were the insurance agents from Ahmedabad, Vadodara and Nashik. They were added to the research field so that personal data being collected, stored and processed with insurance agencies can be tested. Three agents from each city were selected through random sampling method. Questionnaires were mailed to the agents for the research.

Interview method is also employed by the researcher for some call centres. As the manager of international call centre was interviewed by the researcher. The questions of the interview were same as the questions of the questionnaire. The detailed analysis of the data collected from each field has been discussed at length in Chapter 5 of the thesis.

8. UTILITY OF THE RESEARCH

This research would be helpful in creating awareness about importance of data and its protection. The study would also be helpful to many students, teachers and professionals in having a understanding of this area in a better way. This research would be well-intentioned and would turn out to be beneficial reference material for individuals interested in the data protection.

9. SCHEME OF STRUCTURE OF THE THESIS

The research is arranged into six chapters covering the various aspects of data protection. Each chapter brings awareness towards the data protection which starts which general introduction and main content of the chapters.

Chapter one deals with the introduction to the research work done, research aims and objectives along with research methodology and the structure of the thesis. And lastly the output of research is also given in this chapter.

Chapter two shows the historical background of the data protection i.e., how data protection started marking its existence in the world. The evolution of data protection legislation in European Countries, USA and India is discussed at length in this chapter.

Chapter three focuses on Regulatory Provisions related to data protection in the countries like European Union and USA. What are provisions of the data protection legislation followed by these countries are being discussed in this chapter.

Chapter four enlightens the Regulatory Framework of the data protection in India i.e., presently how data protection is dealt with in India.

Chapter five compares the Legal Framework related to data protection of India with the Legal Frameworks related to Data Protection of European Union and USA. The detailed analysis of the data collected by the researcher through empirical research is also discussed in this chapter.

The research work ends with Chapter six which is conclusion and recommendations for the data protection into Indian Context along with a suggested draft bill of Data Protection Legislation inspired by the comparison made in chapter 5 of the thesis as the final outcome of the research

10. ***CONCLUSION***

- To discuss in detail the need for the data protection law with separate entity in India.
- To frame a modified Data Protection Bill that provides wholesome protection to data in India.

11. LITERATURE REFERRED

11.1. Data Protection Directives

Data Protection Directives is like Magna Carta for any law maker framing data protection legislation. The Directives engraves every aspects of data protection into its ambit. The Directives have explicit provisions for what is to be considered as personal data and what is to be included in sensitive personal data. The Directives are guidelines provided to the countries forming European Union. The countries have to frame the data protection legislation in accordance to the Directives. Data Protection Directives are based on seven major issues for data protection which are:

Notice – subject should be notified when and for what purpose their data is collected.

Purpose – data must be processed according to the purpose for which it has been collected and not beyond that.

Consent – taking consent of the subject is crucially important as it is core of the any data protection legislation.

Safeguarding – having appropriate safeguarding measures gives the true sense of data protection.

Disclosure – subject must be informed before the disclosure of his personal data to the third party.

Access – subject must be provided with the right to access for his own personal data so that the accuracy of the data is maintained.

Accountability – data controller must be held with accountability for any loss or theft of the data.

The entire Data Protection moves around the axis of these principals. These are universally referred principals for the data protection.

11.2. Data Protection Law In USA, by Robert Hasty, Dr. Trevor W. Nagel and Mariam Subjally.

This is the article which is published in A4ID (Advocates for International Development). The article gives an overview of how data protection is treated in the United States Of America. It gives a brief idea about sectoral approach taken by the US for data protection. There are no major guidelines given for framing of data protection legislation. The data is divided according to the placement of data. For example health data is protected under separate health insurance portability and accountability act, likewise financial data is protected under the Gramm-Leach-Bliley Act, while children are protected under the Children's Online Privacy Protection Act. Every field of data has a separate legislation which is contrary to the Data Protection Directives.

11.3. Data Protection In India: by Majumdar & Co.

This is an article published by Majmudar & Co. available on www.majmudarindia.com. The article provides picture of the present scenario

for data protection in India. It briefly discusses the legal aspects of data protection in India. It discusses the scattered provisions found under different legislation for the data protection in India.

11.4 India's New Data Protection Legislation, by Raghunath Ananthapur.

This article was published in an online journal called Scripted. The article discusses the Personal Data Protection Bill, 2005. It also discusses the privacy rules taken into consideration under the Information Technology Act along with the grey area left out. The article talks over the Information Technology Act and also critically analyzes it at length.

11.5 Freedom of Speech, The EU Data Protection Directive and the Swedish Personal Data Act.

It is the article that discusses the history of emergence of Data Protection along with the enactment of Data Protection Directives and also the Swedish Personal Data Protection Law. The article is a research based study on the Swedish Law for data protection as some of its provisions are not in accordance to the Directives. The chapter discusses various aspects to be taken into consideration while framing data protection legislation which is important for the research under this thesis.

11.6 Right To Privacy Bill 2010 – A Few Comments, by Elonnai Hickok

This article analyses the Right To Privacy Bill, 2010 put up at Rajyasabha by Rajeev Chandrashekhar. The article gives the detailed analysis of the Bill along with the issues left by the Bill.

11.7 Historical Analysis on European Data Protection Regulations. by

Petra Hoepner, Linda Strick, Martin Löhe.

This article discusses at length the emergence of Data Protection in Europe. The reasons behind the need for legislation for data protection are highlighted in this article. It provides the complete history of the enactment of Data Protection Directives. It also provides information about the committees formed for debating need for data protection in European Union and their reports.

11.8 Analysis of Article 21 of the Constitution- The Expanding Horizons by Vidhan Maheshwari

This article discusses Article 21 (Right To Live) of the Constitution of India as a backbone to Right To Privacy. The article says that right to privacy is covered under the ambit of Article 21 of the Constitution. It discusses the broader view of Article 21 and concludes that right to privacy is one of the fundamental right provided by the Constitution of India.

11.9 Hofstede's Book on Cultural Dimensions.

Hofstede gives an overview of the Indian culture. It was important for the research to study the reason behind such treatment given in India to data protection. According to Hofstede's theory Indian culture is quite distinct from western culture. India has holistic culture, which is a socio-centric concept. In India the relationship of the individual with society is contrary to the western culture. It is observed that in India people living in the society generally trust other people. It is contrary to the individualist societies followed in the western countries. The book gave a clear conclusion about western societies being more aware for data protection rights. According to Hofstede, in India both individual rights aspect of privacy and social value of privacy, are safeguarded.

11.10 Data Governance: How to design, deploy and sustain an effective Data Governance Programme. by John Ladley.

This book is targeted to managers who need to implement a data governance program. It discusses the issues to be taken care of while providing regulations to safeguard data within the control of the managers. The book proposes various aspect on safeguarding data efficiently. The book is useful to the research for the issues that it discusses for safeguarding data.

11.11 History of SSA 1993 - 2000. Chapter 6: Program Integrity. Available at: http://www.ssa.gov/history/ssa/ssa2000chapter6.html

This article provides the history behind granting Social Security Number. It was important to study the reason for which such number is granted so that it can be compared to the Aadhaar number.

11.12 http://timesofindia.indiatimes.com/india/probe-against-3-firms-for-illegal-use-of-aadhaar-biometrics/articleshow/57321007.cms

This new article published in the Time Of India informs about the illegal collection of biometrics under Aadhaar Scheme. The news shows that the Aadhaar Act enacted by the parliament is not providing adequate protection to the data and therefore it has come up that 3 firms were illegally collecting biometrics of the citizens of India.

11.13 http://www.economist.com/printedition/displayStory.cfm?Story_ID=3160118

The news published informs about outsourcing position in India. The discussion going on at Europe and US about not outsourcing data to India as India has no adequate protection standards for data that flows from other countries.

11.14 Aapka Aadhaar. Available at: https://uidai.gov.in/aapka-aadhaar.html

This is website governed by UIDAI and it gives information for registration in Aadhaar scheme. Website provides answers to the questions asked on its site and have all the general information related to Aadhaar.

11.15 The United States Department of Justice, "Overview of the Privacy Act of 1974". Available at: http://www.justice.gov/opcl/social-security-number-usage

The article published on the website provides an overview of the Privacy Act, 1974 enacted at USA. It is said to be one of the first act enacted in the direction of data protection. This law deal exclusively with personal information held by the federal government and do not have any authority over the collection and use of personal information held by other private and public sector entities. The *Privacy Act* was passed in the year 1974 which provided for establishing standards for when it is reasonable, ethical and justifiable for government agencies to compare data in different databases.

11.16 https://economictimes.indiatimes.com/news/politics-and-nation/justice-bnsrikrishna-committee-submits-report-on-data-protection-herere-the-highlights/articleshow/65164663.cms

The article published at the economic times e-paper gives information about the committee formed by government which was headed by Justice B. N. Shrikrishna to lead research into data protection issues. The committee submitted a draft bill on july 2018 for critical acclamation.

11.17 Justice B. N. Shrikrishna Data Prtoection Draft Bill is now public, highlights and What Happens Next – article by Siladitya Ray at Medianama.

Chapter 1
Introduction To The Research

This article gives information about the draft bill. The highlights of the draft bill are noted down. The left over areas of the draft bill is also discussed by the author under this article. The article is published on the website call medianama.

CHAPTER 2

HISTORICAL BACKGROUND OF DATA PROTECTION.

Table Of Contents

1. INTRODUCTION

Data protection has its focus on the individual itself irrespective of the data content and legal constraints. Data security revolves around protecting the integrity and confidentiality of data and is achieved by technical and organizational measures. The Data Protection Act was brought to force for healing such memories of misuse of information.

The first ever computer specified Data Protection Act was enacted in Hesse, in 1970[1]. The misuse of data by the Nazi regime had raised concerns about ability of computers to store and process data along with data protection amongst people.[2] Sweden introduced data protection legislation for a different reason which naturally fitted with two hundred years old system of freedom of information in 1973.[3] It introduced the concept of data subject access to his information stored.[4]

The European Parliament and the Council of Europe on 24 October 1995 adopted its Directive (95/46/EC) for the protection of processing of personal data and on the free movement of such data.[5] The Directives came up as an elaborate data protection structure. The Directive is particularly specific on the transfer of data. It sets down principles concerning the transfer of data to 3rd country. The Directive's major focal point is that the private data of EU

[1]Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG), available at http://www.iuscomp.org/gla/statues/BDSGhtm, visited on 22nd November 2012.
[2] Parag Diwan and Shammi Kapoor., Cyber and E-Commerce Laws with Information Technology Act,2000 & Rules therewith, Bharat Publishing House, New Delhi, 2nd Edition,2000.
[3] Freedom of Speech, The EU Data Protection Directive and the Swedish Personal Data Act, available at www.dsv.su.se/jpalme/society/eu-data-directive-freedom.html, visited on January 21st 2017.
[4] Parag Diwan and Shammi Kapoor, Cyber and e-commerce laws, 2nd ed.,[2000].
[5] Directive 95/46/EC 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, available at http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT

nationals should not ideally be sent to countries that don't meet the EU "adequacy" standards with reference to privacy.[6]

It must be noted that data protection laws were created in 1970ies where computer data was primarily handled by government officials. The international developments gradually showed that the protection of personal data cannot be addressed exclusively at the national level only. At the beginning of the 80ies the Council of Europe and OECD issued standard information for data protection laws. Throughout the 90s, the European "single market" plan emerged to facilitate easier trade. The EU Data Protection Directive (EU DPD) was provided to support single market before internet became common amongst the masses. The development and consequences of data protection are below-

- **1970ies:** The first ever data protection laws were created, when computers were used by few and majorly by government officials. There was a threat that the state, by connecting various registries, would gain an informational superpower over the individual, the motive of the Data Protection Laws was to prevent abuse of non-public information and to confirm the rights of access and rectification. Obligations regarding registering the databases containing personal data were noted in this generation of data protection laws. In 1970 the German Land of Hessen adopted the primary law on the protection of non-public information within the world. It was followed by Sweden (1973), Germany (Federal Act, 1977), France (1978) and other countries. Three countries included data protection among their constitutionally guaranteed rights (1976 Portugal, 1978 Spain and 1978 Austria).[7]
- **1980ies:** The international developments, however, step by step showed that the protection of non-public information cannot be managed

[6] Directive 95/46/EC 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, available at http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT

[7] A historical overview on the information technology developments and its implication on data protection legislation is given by the dataprotection.eu.

completely at the national level. At the starting of the 80ies the Council of Europe in conjunction with the OECD issued data protection regulations. At this time cross-border flows of personal data could be considered as discrete events, with data travelling in bulk between identified parties. Data transfers would occur, in massive batches with use rudimentary physical devices like tapes for processing information. International data banks were simply rising, and the web was in its starting phase therefore there were some prohibitions on business use. In 1983 the German Federal Court declared that it was a basic right of individuals to see how their data was being used. This information was self-determined and concentrates on the specific rights for the individual concerning the whole system of personal data processing and influenced the data protection legislation in the following years. The Single European Act was signed in 1987 with the gradual move towards a "single market" for trade. The elimination of boundaries between eastern and western Europe i.e., the Berlin Wall further unified Europe in 1989.[8]

- **1990ies:** Throughout this period, the "single market" plan emerged to support easier trade. The EU Data Protection Directive (EU DPD) was formulated before the World Wide Web was invented and hence it was designed for a world in which data processing took place in comparatively few, easily identifiable locations, usually with mainframe computers. The technological changes of the period – the appearance of personal computers, and their subsequent connection to networks – decreased the regulation of technology. Regulations became increasingly abstract and less technology-specific. Computing moved from being a single computer to a globally connected network of computers. New principles (e.g. data economy by a minimum processing of personal data in the German Tele Services Data Protection Act 1997) were enacted as the internet grew more and more powerful.

- **Since 2000:** New technological developments like cloud computing and social networks etc. occurred since Directive 95/46 was adopted. New

[8] A historical overview on the information technology developments and its implication on data protection legislation is given by the dataprotection.eu.

internet corporations entered the arena such as Google, Facebook, Twitter, Skype etc. This lead to a gradually rise of easier cross border information transfers. With rise of technology and consecutive data flows, there was also a rise in using internet for purposes of terrorism, anti-social activities, forms of international organized crime etc., which has resulted in an increase in international judicial activities supported by enormous exchange of information for law enforcement (Hustinx 2011). These developments caused the revision of the EU Data Protection Directive as communicated in European Commission 2010b.[9]

2. HISTORICAL BACKGROUND OF DATA PROTECTION IN EUROPEAN COUNTIRES

Referring to the experiences under World War II era the extensive European privacy regulation can be justified. Europeans were a bit apprehensive of unchecked use of personal information. World War II and the post-War period was a time in Europe that disclosure of race or ethnicity led to secret denunciations and seizures that sent friends and neighbours to work camps and concentration camps. With the technological leaps, Europeans started taking data protection seriously.[10]

European countries were the chief countries to adapt and frame laws concerning the protection of personal rights of someone. The historical root of the EU lies within the Second warfare. After the war, Europe had split into East and West. Six West European nations created the Council of Europe in 1949. It was a primary step towards getting much needed unity amongst them. Gradually began the formation of the European Union which was noticed first as a trading group. In 1957 six countries signed the Treaties of Rome in effect making the European Economic Community (EEC), and also

[9] A historical overview on the information technology developments and its implication on data protection legislation is given by the dataprotection.eu.

[10] The History of the European Union, available at http://europa.eu/about-eu/eu-history/index_en.htm, visited on 17th November 2015.

establishing central union by removing customs duties on product imported from one another and allowing free cross-border trade for the first time. In 1987, the Single European Act was signed with the intention to finish the solo market by 1992. There was a steady increase in countries joining as member- 1973: nine countries, 1986: twelve countries, 1995: fifteen countries covering nearly the full of Western Europe, 2002: twenty five countries, 2007: twenty seven countries.[11]

The European Union was officially recognised only when the Maastricht Treaty came into force on 1 November 1993. Maastricht Treaty officially replaced the name European Community to European Union.[12] The main aim of establishing European Union was to unify Europe in additional ways beyond trade, having unified rules all over, having single currency and additionally for foreign and security policy along with unity in justice and home affairs. In 2002, Euro was introduced as common currency amongst the public of European Union. By 2007, twenty-seven EU countries signed the Treaty Of Lisbon, which basically amends the previous Treaties. It enhanced the democracy, efficiency and transparency of European Union. It mandates that the EU Parliament and Council supply norms for data protection within the public and non-public (private) sectors. Article 16 of European Union 2008, gives the right of individual's personal data to be protected.

2.1 COUNCIL OF EUROPE

The Council of Europe[13] was incorporated in 1949 post World War II by 10 European countries and now covers whole European continent, with 47 member countries. It strengthens democracy, human rights and the rule of law throughout its member states, it was one of the major task of Convention 108. It was affirmed in the 'European Convention for the Protection of Human Rights and Fundamental Freedoms" (1950), that each individual has right to

[11] The History of the European Union, http://europa.eu/about-eu/eu-history/index_en.htm, visited on 17th November 2015.
[12] International Relations, fourth edition book by Peu Ghosh published by Eastern Economy Edition.
[13] Council of Europe, http://www.coe.int, visited on 2nd June 2016.

private life and personal communications without any state interference.

As automatic processing became more relevant during the 70ies this led in 1980 to the "*Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data*" (also called Convention 108).[14] The Council of Europe worked in conjunction with OECD in the late 1970ies and in January 1981 Convention 108 was opened for signature. OECD, along with additionally four of its non-European member countries (Australia, Canada, Japan and also the United States) placed a proxy observer on the Council of Europe's committee formulating the Convention.

The Convention was the first legally binding international instrument in the data protection field only for the countries that ratified it. According to the Convention, the parties wishing to ratify with the convention were required to amend their national legislation in conjunction with the principles laid down for processing of personal data. The Convention outlined the fundamental privacy principle for automatically processing of personal data that are –

1. gathered and consecutively processed in a legal manner;
2. stored for specific and legal purposes only and not any other interests;
3. adequate, pertinent and appropriate information must be stored for achieving the said purpose;
4. accurate and up to date with latest data;
5. the identifiers factors of the data should not be stored for longer than what is required.[15]

Beyond this personal data needs to be safeguarded so it can be amended or erased later on. Processing of 'sensitive' data eg race, colour, health,

[14] Council Of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, (ETS No. 108), Strasbourg, 28/1/1981, available at http://conventions.coe.int/treaty/en/Treaties/Html/108.htm
[15] Council of Europe, available at http://www.coe.int, visited on 2nd June 2016

religion, criminal record, etc. are also covered under this when no other legal provisions are there. Certain restrictions are imposed on trans-border flows of personal data to states where legal regulation does not provide equivalent protection by the Convention.[16] The principles have inherently become foundation of privacy laws frames subsequently across Europe.

2.2 SAFE HARBOUR

As per Article 25 of EU Data Protection Directive, Member states are not allowed to transfer any data to external countries till the time they are not assured of adequate data protection laws in it. However, there is no clear mention on what is meant by 'adequate protection' in the Directive.[17]

US and European Commission began their discussion over trans-border flow of data with the goal of ensuring high data protection standards while maintaining the free flow of data across the Atlantic much before EU DPD came into force. Regulations surrounding trans-border data flow were discussed between US and EU which revolved around 3 major pointers-

1. Individual control over uses of personal data
2. The amount of protection needed to ensure before transfer of personal data.
3. Nature of enforcement authority.

This led to the formulation of "Safe Harbour" principle which was in compliance with EU data protection directives.[18] Such arrangement which was agreed upon by US businesses would be viewed as being in compliance with the adequacy requirement of the EU Directive. The concluding approval of

[16] Historical Analysis on European General Data Protection Regulations, published by European Data Protection Supervisor.
[17] Historical Analysis on European General Data Protection Regulations, published by European Data Protection Supervisor.
[18] Press release European Commission, Data protection: Commission endorses "safe harbor" arrangement with US, 29 March 2000, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/00/301&format=HTML&aged=0&language=EN&guiLanguage=en, visited on 12th April 2018.

'Safe Harbour Privacy Principles' were released in July 27th, 2000. In order to meet the EU "adequacy" standards, US developed a 'Safe Harbour' framework, according to which the US Department of Commerce would maintain a list of US companies that have been self-certified to the safe harbor framework. It may be noted that subscribing to the Safe Harbour Initiative remains voluntary to the corporates. The legal enforcement power of these principles is governed by the Federal Trade Commission. [19]

3 HISTORICAL BACKGROUND OF DATA PROTECTION IN UNITED STATES OF AMERICA

United States and the E.U, focuses on data protection. However, both their approaches are different. In the U.S data is segregated into different types according to their use and sensitivity.[20] The government awards a certain level of protection to each class of data. [21] Beyond the constitutional interpretations given by the court and international treaties, there are many other laws that deal only with data protection. While discussing history of data protection in USA, the **Privacy Act of 1974** and the **Computer Matching and Privacy Act** were the first laws which dealt with the data stored by the government and do not govern data held by other corporates or ancillary government entities.

The Privacy Act set out standards for government bodies to guide them as to when it was legal to analyse data in different databases. *The Privacy Act of 1974* along with the company of **Freedom Of Information Act (FOLA)** of 1966 provided the people right to access government information. However, it

[19] Book on The Regulation Of Privacy And Data Protection In The Use Of Electronic Health Information, by R. J. Rodrigues, P. Wilson and S. J. Schanz, published by PAN Health Organization.

[20] CYBER TERRORISM – A Project Report submitted in partial fulfilment for the award of the Degree of Masters of Computer Applications in Department of MCA by Ankita Jain submitted at Govt. Mahila Engg. College, Ajmer.

21 Data Protection Law In India by Pankaj Kumar - Student of 4th year student, Bangalore Institute of Legal Studies, published on website of Legal Service India (Website for Lawyers), available at http://www.legalserviceindia.com/article/l37-Data-Protection-Law-in-India.html, visited on November 13th 2012.

had its exceptions such as employee records and medical files were not freely accessible as they would cause a breach to privacy. People's request to access their own records was initially denied under this provision. Privacy Act was an open statute which gave people the right to get their information as well as protect information in government databases. [22] The act was developed explicitly to address the problems posed by electronic technologies and personal records systems and covers the vast majority of personal records systems maintained by the federal government. The act set forth some basic principles of "fair information practice," and provided that people could now challenge their information present in government databases. However, Information could only be disclosed by the consent of the person it concerns.

Additionally **The Computer Security Act** of 1987 also governs personal records of people kept by the government systems. The Act formulated standards for computer security and assigns responsibility for those standards to National Institute of Standards. The law beyond that implores the government to identify the most sensitive systems and formulate appropriate safeguards regarding them.[23] The **Computer Matching and Privacy Protection Act** of 1988 was an updated version of the Privacy Act and it had new provisions that governed computer matching primarily. Computer matching refers to the process with which a common comparison is used to match up information about a person from various sources in order to see if the person qualifies for certain government benefits.

The **Electronic Communications Privacy Act** was formulated to restrict surveillance of electronic communication as well as prohibiting access to stored data without consent of the individual or the service provider at large. The **Children's Online Privacy Protection Act** was enacted in 1998 which mandated that website controllers took requisite permission from parents of

[22] Web 20 (Social Media) Policies in Higher Education, by Anne Arendt, Utah Valley University, published on 6th November 2009, available at https://www.slideshare.net/annearendt/web-20-social-media-policies-in-higher-education.

[23] 'Data Protection and Privacy in the United States and Europe', by J.S Stratford, Yale University. New Haven, Connecticut: University of California, published in IASSIST Quarterly.

children before gathering any information about them. The **Consumer Internet Privacy Protection Act** required an ISP to get permission of the subscriber before disclosing his personal information to third parties.[24] The **Video Privacy Protection Act of 1988** amended the Federal Criminal Code and it restricts any disclosure of records of video rentals containing any identifiers of personal information. Any individual who believes their rights were violated can challenge it in civil court under this act for damages as well as destruction of his /her records after a frame of time.

There are many other laws concerning data protection. Those laws are the one is concerned with the data held by government. Generally, laws provide explicit declaration regarding types of data and best practices to deal with such data is to ensure their optimum protection. Some of these laws only allow information to be disclosed to Census officials. Data with the national health centre can only be used for any research purposes without any exceptions.

The **National Education Statistics Act** re-authorized and rectified the provisions of the National Centre for Educational Statistics and the National Assessment of Educational Progress. The confidentiality and distribution processes were changed after this law was enacted. The **Tax Reform Act** mandates that financial information eg tax returns, gross income etc need to be kept confidential. The act permits only limited disclosure of returns and returns information for specific purposes, and specifies procedures for disclosure. It specifies the punitive actions possible in case one violates any of the clauses and does an illegal disclosure of such information. The victim can take civil action for damages and also criminal penalties are established for wrongful disclosures under the act.

The **Fair Credit Reporting Act** governs the use of financial data by consumer credit reporting agencies. They should always assure that

[24] Web 20 (Social Media) Policies in Higher Education, by Anne Arendt, Utah Valley University, published on 6th November 2009, available at https://www.slideshare.net/annearendt/web-20-social-media-policies-in-higher-education

information supplies by them is completely accurate, relevant to the purpose for which it is used and at the same time appropriate privacy rights of the individuals are maintained at all times. With evolving technologies, even the field of data protection is getting more refined and new laws are being made to address the new rising issues.

4 HISTORICAL BACKGROUND OF DATA PROTECTION IN INDIA

Before the Constitution of India was enacted in the year 1950, the state did not grant any guarantee for rights to the citizens. The enforcement of Constitution provided the status of citizens to the people of India. After the Constitution came in force, there was no explicit guarantee of fundamental provision concerning the right to privacy. The Constitution of India, mentioned the Fundamental Rights in part III enumerated in Article 14-30. Judicial activism brought right to privacy as part of the Fundamental Rights.

Right to privacy was deduced to Right to Life and Personal Liberty enshrined under Article 21 by the Supreme Court through an extensive interpretation of the phrase *Personal Liberty*.[25] Article 21 mentions that nobody should be allowed to deprive anyone else from their fundamental rights and law should be followed at all times.[26] Taking this provision as a baseline, the Supreme Court observed that "those who deprive other persons of their personal liberty in discharge of their duty must strictly observe the rules of law". Therefore according to the Supreme Court "Personal Liberty" can be viewed as life free from abuses not sustainable in the eyes of law.

Since the Constitution came into force, Indian judiciary deals with

[25] Article 21 of the Constitution - Protection of life and personal liberty.- No person shall be deprived of his life or personal liberty except according to procedure established by law.
[26] Indian Public Administration: Institutions and Issues, by Ramesh K. Arora and Rajni Goyal, published by Wishwa Prakashan.

privacy concerning issue either under the light of fundamental rights or under the common law jurisprudence. Privacy was never provided equal rights as given to the other fundamental rights of the Constitution. The judiciary does not have extensive experience in dealing with issues concerning privacy rights. Decisions concerning it are done on a case to case basis.

The first case which was indirectly related to privacy issue was noted in **Kharak Singh v. State of Uttar Pradesh**[27], where the Supreme Court comprised of seven judges bench was to make a decision on whether the police was right in undertaking surveillance of people with a criminal records and making domiciliary visits. In this case the concerned individual was being troubled by the police who made visits at night under the Regulation 236(b) of UP Police Regulation, which permits domiciliary visits at night. The individual challenged it in court stating that they were a violation to his own liberty granted under the 'personal liberty' of Article 21. The majority of judges objected stating that right to privacy was not part of the fundamental rights granted to the citizens. However, the judges opined that right to privacy can be considered under the common law right of citizens. Only two judges out of seven agreed that irrespective of the position of right to privacy in the Constitution, it still was a basic right which granted liberty. Justice Subba Rao held "It is true our Constitution does not expressly declare a right to privacy as a fundamental right, but the said right is an essential ingredient of personal liberty." [28]

Again the issue of privacy was raised at the Supreme Court in **Govind v. State of Madhya Pradesh**. In this case, the petitioner challenged certain police actions for violating his right to privacy. Again, only three judges of the bench were inclined to interpret it in view of a right to privacy. One of the judges argued that a person's life was free from official intervention in all things except when it was not reasonable to do so. Justice Mathew stated: "Rights and freedoms of citizens are set forth in the Constitution in order to guarantee that

[27] AIR 1963 SC 1295
28 Kharaksingh V. State Of Uttar Pradesh ((1964) SCR (1) 332)

the individual, his personality and those things stamped with his personality shall be free from official interference except where a reasonable basis for intrusion exists. 'Liberty against government' a phrase coined by Professor Corwin expresses this idea forcefully. In this sense, many of the fundamental rights of citizens can be described as contributing to the right to privacy."[29]

In the case of **R. Rajagopal v. State of Tamil Nadu**, the right to privacy and right to freedom of speech were seemed contradicting with each other. In this case, the petitioner was a news magazine based in Tamil Nadu had sought directions from the Court to restrain the State of Tamil Nadu and its officers from interfering into the publication of the autobiography of a death row convict–'Auto Shankar'. The state and its officers tried to restrict the publication as it contained details about the nexus between criminals and police officers. The Apex Court had to deal with the issues like: "Whether a citizen can prevent other citizen from publishing his biography? Does the freedom of speech and expression guaranteed by Article 19(1) (a) entitle the press to publish such unauthorised account of a citizen's life and activities and if so to what extent and in what circumstances?" The Supreme Court comprised of two judges bench, for the first time was of the opinion that Right To Privacy should remain at individual level and should not be mixed with matters of a public domain. The Supreme Court states-

- "Right to life and personal liberty guaranteed to the citizens by Article 21 covers right to privacy into it. Right to privacy can also be viewed as a "right to be let alone". As per Article 21, an individual can grant right to privacy to safeguard privacy regarding marriage, family motherhood, education, etc. Nobody is authorized to publish anything regarding it regardless of the content. If someone does so, then it would be a clear violation of right to privacy of the person concerned and would be liable in an action for damages. Unless a person gets into a controversy, and matters related to him/her come out in the public domain then things will be different.

29 Govind V. State Of Madhya Pradesh (AIR 1975 SC 1378)

- The rule aforesaid is subject to the exception, any publication which publishes certain things which are based on publicly verifiable records and court cases, then, it will not be considered as a breach to privacy. It states that once a matter comes into the public domain , it no longer remains private and is free to be commented upon by the press, critics etc. at their own discretion."[30]

Though it is expected that the intelligence cell of the government will try to gather information using such means, however it is an invasion to the individual's life. It would be a clear violation of Article 21 of the Indian Constitution.

In the case of (People's Union for Civil Liberties) **PUCL v. Union of India**[31], the issue of unauthorized tapping into phone calls was raised. The court was of the opinion that tapping telephone calls was a serious breach of individual's privacy. It is undoubtedly correct that every government, democratic or not, exercises some degree of sub rosa operation as a part of its intelligence outfit, but at the same time citizen's right to privacy has to be safeguarded from being abused by the authorities. Telephone-tapping would, thus, infringe Article 21 of the Constitution of India unless it is permitted under the procedure established by law."[32]

In the case of **Pooran Mal v. Director of Inspection (Investigation) of Income-tax**, **New Delhi,**[33] the court categorically states that searches done by the government body to gather evidence would not be a violation as there is no fundamental right to privacy.

In the case of **Mr. 'X' v. Hospital 'Z'**[34], the Supreme Court was the

30 R. Rajagopal V. State Of Tamil Nadu (1994 SCC (6) 632)
[31] (1997) 1 SCC 30
32 PUCL v.s Union of India ((1997) 1 SCC 30)
[33] AIR 1974 SC 348
[34] AIR 1999 SC 495

questioned of blood donor's right to privacy of medical records. The relationship between doctor and patient is a professional one as there is a trust which is established in it. Doctors need to ethically maintain confidentiality. There are some situations where public interest is given more importance than client confidentiality. Right of Privacy which may at certain point of time clashes with one person's "right to be let alone" with another person's right to be informed. For example, in situations such as criminal cases or situations where there is a threat to widespread health risk for all citizens. In this case, the hospital had disclosed that the person was diagnosed with HIV without his consent. Due to this the lady who was supposed to marry this person broke off and the petitioner also faced social harassment. The Apex Court in this case gave the verdict that medical records are private but doctors and hospitals could make exceptions in certain cases when non-disclosure can endanger the lives of other citizens.

In the case of **District Registrar vs Canara Bank**[35] case, the court had to judge the A.P Stamps Act, which inherently allowed the collector or any authorized person by the collector to enter any premises and conduct inspection of books, document etc., if this would help in the discovery of fraud or omission of any duty payable to the government. The issue was critical as it related to the data held by a financial institution like the bank. The court held that such an inspection clearly violated the in Articles 14, 19 and 21 of the Constitution as it failed test of reasonableness.

The Supreme Court stated that any such test should satisfy three main tests to be considered as per constitution as stated in the **Maneka Gandhi v. Union of India**. The triple test addresses the concept of personal liberty with respect to Article 21 –

- "It should be an established procedure.
- The procedure should in principle be compliant with one or more fundamental rights conferred under Article 19 concerning the situation.

[35] ((2005) 1 SCC 496)

- It must also be tested under Article 14."

Most importantly, the Court ruled that the concept of privacy related to the citizen and not the place. Therefore, whether the financial data was kept in home or at the bank, the mere fact that the data was of private individuals guarantees protection under national law at all times. As long as the financial records of the citizens are concerned, those records would be protected under the citizen's right to privacy.[36]

In the case of **Peoples Union for Civil Liberties (PUCL) v. Union of India**[37], the right to privacy was not violated when criminal records regarding an electoral candidate were published. It was determined that the rights of people to know the candidate's history were more vital than the right to privacy of the electoral candidate.[38]

Post the year 2000, there have been more revisions made in law to bring stored electronic data (especially private data) into the ambit of IT Act, 2000 for data protection. These revisions resulted into the addition of certain provisions which provided protection of stored data for the first time. The Personal Data Protection Bill presented in 2006, was considered to provide protection to the personal information of the individual. Another Bill called the "Right To Privacy Bill" was presented consecutively at the Parliament as a second attempt towards specific law for data protection.

36 District Registrar v. Canara Bank ((2005) 1 SCC 496)

[37] AIR 2003 SC 2363

38 Peoples Union for Civil Liberties (PUCL) v. Union of India, AIR 2003 SC 2363

CHAPTER 3

REGULATORY FRAMEWORK OF DATA PROTECTION IN EUROPEAN UNION AND USA

Table Of Contents

1. INTRODUCTION

The United Nation Declaration of Human Rights (UDHR) of 1948 which was the foremost statute in the data protection field laid out provisions in Article 12, for an individual's right to maintenance of his/her private life without any sort of interference from external agencies, included but not limited to the state.[1] The UDHR helped give guidance to lawmakers while framing policies regarding human rights in Europe and in other geographies globally. With the rapid growth of technology from the 1960s, there has been a pressing need for framing laws surrounding the protection of personal data of individuals lying with government bodies and global corporations. The misuse of such personal data could lead to catastrophic effects on individual's present and future.

Looking at the data protection legislation prevailing in USA and EU nations, there is difference which is quite noticeable about the perception of privacy amongst these countries. For Europeans privacy protections is a right to respect and have personal dignity. The core of European privacy rights is rights related to one's image, name, and reputation, and what Germans take up privacy rights are the right that control the kinds of information disclosed about oneself. As per the European concepts of privacy : Privacy includes all rights to control your public image, rights to guarantee that people see you the way you want to be seen. EU countries consider privacy rights as rights to be shielded against unwanted public exposure to escape embarrassment or humiliation. Media is considered as the major enemy of privacy because it always threatens to broadcast such information about oneself in ways that endanger one's public dignity. Any other agent that gathers and disseminates information can also pose such dangers.[2]

Contrast to this is the American notions of privacy. America is much more concerned with ideas of liberty, and especially liberty against the state. The Americans

[1] United Nations (UN), Universal Declaration of Human Rights (UDHR), 10 December 1948, available on www.un.org

[2] The Two Western Cultures of Privacy: Dignity Versus Liberty. By James Q Whitman.

sticking to its stand taken in 18th century considers right to privacy as the right to liberty from intrusions by the state, especially in one's own home. According to the American Supreme Court's opinion about privacy as it stated in 19th century: The prime danger, from the American point of view, is that "the sanctity of privacy will be breached by government actors." American concerns thus emphasis relatively less on the media. Instead, they lean towards to be concerned more about preserving a sort of private independence within their own walls.[3]

2. U.S. DATA PROTECTION LAWS

"Privacy" as a term is not explicitly mentioned neither in the U.S. Constitution nor the Bill of Rights. However, the U.S. Supreme Court has at various times in the past recognised the right to privacy deriving it from historical Amendments such as the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments. The Supreme Court took cognizance of the right to privacy way back in 1977 in *Whalen v. Roe* case. It fundamentally agreed that the Constitution was entrusted with two major responsibilities. One was to recognize the interest of an individual in not disclosing matters of a personal nature. Beyond that, it was also responsible for protecting the interest of an individual in making requisite decisions independently. As far as data protection is concerned, historically there have been a number of laws tackling the concept of data protection and a range of ancillary issues. The Universal Declaration of Human Rights (UNDHR), United Nations International Covenant on Civil and Political Rights and numerous interpretations provided by the court are just some of the legal foundations which have helped shaped future statutes on data protection.

Although there is no individual law that governs the treatment of data protection or privacy, the United States data protection law currently enforced is an amalgamation of federal laws and state regulations. This is supposed to provide overall guidance on

[3] The Two Western Cultures of Privacy: Dignity Versus Liberty. By James Q Whitman

the storage and use of private data by corporations across business verticals. There is, however, a clear demarcation between the state and federal laws governing power. While the federal law is fundamentally based on the principles regarding the collection, storage and use of confidential public information, the state law requires a mandatory public disclosure by agencies and corporation whenever any security breach which endangers leak of non-public information has taken place. It is important to note that both state and federal statutes can be enforced through civil suits filed by citizens. In normal practice, federal statutes are enforced by the federal government and state laws are enforced by the state regulators. [4]

2.1 FEDERAL STATUTES

Multiple statutes have been enacted under the federal government of United States. These are as follows-

2.1.1) Federal Trade Commission Act

Federal Trade Commission Act (FTCA) was enforced to prevent any malpractices which would have a dire effect on the economy. Federal Trade Commission has also reprimanded companies where it felt that the companies did not protect consumer data as per their stated privacy policies. FTCA has monitored and ensured strict compliances of privacy policies by companies to prevent any illegal leakage of confidential consumer data.[5] The FTCA has also questioned companies that were disclosing consumer data beyond the limits of their privacy policy clauses.[6] Companies seeking FTCA compliance are advised to stay within the norms prescribed in their privacy policy and not breach it for any ancillary commercial interests as consumer data by its nature is inherently sensitive and critical.

[4] Data Protection Law In USA, by Robert Hasty, Dr. Trevor W. Nagel and Mariam Subjally, available at www.neighborhoodindicators.org

[5] Decision and Order, Petco Animal Supplies, Inc., FTC File No. 032-3221 (2004) available on www.ftc.gov

[6] FTC v. Rennert, International Outsourcing Grp., Inc., et al., CV-S-00-0861-JBR (D. Nev. 1999) (FTC File No. 992-3245), available on www.ftc.gov, visited on 8th March 2015.

2.1.2) Family Educational Rights and Privacy Act

The Family Educational Rights and Privacy Act (FERPA)[7] were originally formulated keeping in mind sensitive student academic records which are in hands of numerous educational institutions that receive monetary assistance from the government. Educational records mean any and every information possessed by an educational institute comprising of the student. Educational institutes may be any private or public educational body which receive government monetary assistance.[8] Under this statute, once a student of such an educational institute reaches eighteen years of age, parents can inspect any past educational record of the student if they wish to. Every educational institute is required to establish appropriate procedures for granting such requests within a reasonable time. Such institutes are mandated to have fixed procedures in order to release requisite documents in a reasonable time frame. According to this statute, the educational institute needs to have a written permission from the student's guardians or the student, before releasing such data to them.

Beyond that the educational institute is also required to keep a record of any individual or companies that have in the past requested a student's data. These records can only be disclosed to the parents/ school senior staff and staff that manage the recordkeeping process. It is important to note that such data can readily be transferred to any external party on the condition that it takes the written consent of the student/parent before giving out the data to any other company. The provisions of the FERPA may be enforced by the Secretary of Education.

2.1.3) Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act (COPPA)[9] was enacted to safeguard Internet usage by kids below thirteen years of age. The statute regulated how websites are collecting, protecting and using the data obtained from kids. This statute makes its

[7] 20 USC § 1232g, available at www.gpo.gov, visited on 14th March 2015.
[8] 20 USC § 1232g(a)(1)(D)(3) available at www.gpo.gov, visited on 14th March 2015.
[9] 15 U.S.C. §§ 6501, *available at* www.coppa.org, visited on 27th March 2015

mandatory for websites to notify and take consent of the parents before accumulating data of kids. It should also disclose its data collection practices in a transparent manner. This statute is aimed at both, websites where the target audience is children and generic websites where information of kids will be collected. From 2013, personal information's scope was widened to include other vital details such as geo-location data and any information transferred by way of cookies while using the website.

2.1.4) Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) covers primarily institutes which actively collect, store and use specific personal health data of individuals. These include all ancillary parties too eg drug stores, insurance companies etc[10]. Such entities need to comply with the below rules-

1) PrivacyRules.
2) Security Rules

Privacy Rules prohibit any disclosure of Confidential Health Information of patients unless it is for some adhoc situations or explicitly authorized by patient. Security Rules specify that such entities need to have proper policies and standard operating procedures for the collection, storage and usage of confidential Health information. These rules were revised in 2013 as part of the HIPAA "Omnibus Rule".

Another similar statute called the Health Information Technology for Economic and Clinical Health Act (HITECH) also pertains to personal health information.[11] The HITECH Act primarily focuses on corporates that work in tandem with health institutes. These may be companies that work on behalf of health institutes or alternatively companies that assist health institutes in their proper usage and disclosure of any such confidential health information. This makes such corporates equally responsible for complying with Privacy and Security Rules. Any defects observed in compliance of the

[10] www.legalarchiver.org, visited on 4th October 2017.
[11] www.healthit.gov, visited on 18th February 2013

same will make them liable for legal prosecution for failing to deliver their duties of stewardship of confidential health data.

2.1.5) Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)

The Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)[12] is primarily concerned with regulating commercial emails. These emails are promotional mails which seek to advertise products or services of a commercial nature.[13] Personal emails are not covered under this law. This law prohibits companies from sending any inaccurate or deceptive advertisements to lure the target audience. Beyond this the providers also need to ensure that they give an opportunity for the email recipient to unsubscribe from the email messages without any obligations. The emails should also have the physical mailing address of the company in the email message. The senders must respect the decisions of recipient's unwillingness of receiving any such future emails from the sender. This Act is legally enforced by the Federal Trade Council (FTC).It may also be noted that State Attorney Generals can also enforce this statute as it is a violation of state laws preventing such type of electronic promotional messages.

2.1.6) Fair Credit Reporting Act

The aim of introducing the Fair Credit Reporting Act (FCRA) was to fundamentally ensure that credit reporting is done both fair and accurately as it concerns financial matters.[14] The Act through its provisions also gives proper guidelines regarding the accumulation, storage and use of such data held by "Consumer Reporting Agencies" shared through the issuance of Consumer Reports. These agencies primarily collect information and analyze it and thereafter forward it to a third party. [15] According to this statute a consumer report contains all factual information to determine an individual's

[12] 20 USC § 1232g(a)(4)(B) available at www.gpo.gov, visited on 18th February 2013
[13] 20 USC § 1232f available at www.gpo.gov, visited on 12th June 2017
[14] 15 U.S.C. § 1681, *available at* www.ftc.gov, visited on 10th January 2015.
[15] 15 U.S.C. § 1681a(f), *available at* www.ftc.gov, visited on 10th January 2015

historic repayment track and other lifestyle factors which will be analyzed as per requisite processes before granting any credit or insurance approval.[16]

According to this law the Consumer Report should not be used for any advertising purposes unless-

- The consumer is informed in advance that their information will be shared publicly
- The consumer did not use his chance to opt out of the marketing.

The consumer should be given adequate time to opt out of such marketing. Once opted out they will be free from any such promotional messages for at least 5 years. Companies are legally bound to give customers a facility to opt out and give adequate warning in case they are disclosing any personal credit information. When a corporate discloses information to other affiliates without complying with the law, both the company and its affiliate are liable for prosecution under FCRA.

2.1.7) Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA)[17] makes it compulsory for financial institutions to safeguard the confidential non-public information of its consumers. [18] Here the term 'financial institutions' represents institutions such as banks, insurance firms, security companies and other related companies that are involved in providing products and services of financial nature to the public. Non-Public Personal Information represents all personally identifiable information which is given by the customer to such an institute while availing any product/service. It also includes information obtained from other sources.[19]

[16] 15 U.S.C. §§ 1681a(d)(1), 1681a(f), *available at* www.ftc.gov, visited on 10th January 2015
[17] 20 USC § 6801 available at www.gpo.gov, 4th November 2015.
[18] 20 USC § 6801(a) available at www.gpo.gov, 4th November 2015.
[19] 20 USC §§ 6809(4)(A)(i)-(iii), *available at* www.gpo.gov. 14th March 2015.

To ensure strict compliance of the Gramm-Leach-Bliley Act, financial institutions must disclose-

1. Its internal policies and procedures concerning handling of non-public information in both kinds of companies – affiliated and non-affiliated.
2. The wide spectrum of non-public information that such an institute collects as part of normal course of business.
3. Policies to safeguard such information. Such institutions should disclose its privacy policies at the starting itself to the customer. They should also give them an option to deny sharing of such information to any third parties. Third parties should be furnished with the privacy policies of the company every year. [20]

The financial institution must clearly disclose their privacy policy at the time of establishing relationship with the consumer. In addition, financial institutions are required to provide customers with annual notice of their privacy policies and of the right of unwillingness from sharing personal information with non-affiliated third parties. The third party which maintains an ongoing relationship with the consumer who agrees to disclose their non-public financial information to them should be provided copies of the organization's privacy policy annually.

Financial institutes should keep in mind below points to remain compliant of the Act-

- A designated employee should be assigned with the duties of maintaining the information security program.
- Internal procedure to be established to combat any risks to such vital information and necessary controls to be put in place for it.
- Ensure all service vendors are contractually bound to protect such information.
- Modify the information security program as and when needed.[21]

[20] 20 USC §§ 6803(c)(1)-(3), *available at* www.gpo.gov, 14th March 2015.
[21] 15 U.S.C. § 6805(a), *available at* www.gpo.gov, 14th March 2015.

Unlike many other acts, this statute can be enforced only by government bodies. Apart from these policies there are other such rules also to ensure privacy such as Safeguards rule, Disposal Rule and last but not the least- the Red Flag Rule which covers financial data and is officially regulated by the FTC.

2.1.8) Electronic Communications Privacy Act and Computer Fraud and Abuse Act

The Electronic Communications Privacy Act deals with electronic communication. Likewise, the Computer Fraud and Abuse Act, deals with any illegal tampering of IT devices to serve any ulterior motives. In 2008, such a fraud was reported and a particular internet service provider working in tandem with an advertising company captured data emanating from individual computers and their respective ISP servers.

2.2 STATE STATUTES

Majority of the states in U.S.A have recognized the need for data protection and have accordingly formulated laws. Moreover, Federal Laws are also applicable along with the State laws for the data privacy protection in the states which have enacted data privacy laws. Hence one cannot strike a difference in the applicability of the Federal and State Laws. The Federal and State Laws are sets of laws that would be applied in concert with each other. While State Laws are limited in terms of the geographical state that they cover, federal laws are applicable throughout the nation. State laws generally require corporates to disclose any breach of data to the public. Beyond this, the customers who have been affected by the data breach need to be informed within reasonable time. It may be noted that few states have relatively more advanced laws when it comes to data protection such as California and Massachusetts. It is important to note that California and Massachusetts enacted laws that apply to any entity, in whole United States, with access to non-public information of any of their residents.

2.2.1) New York Data Privacy Laws

1) Information Security Breach and Notification Act

The New York General Business Law clearly states that any company in New York that owns or licenses for specific computer data which also has private information of the resident of New York, is also responsible for disclosing any breach of data by illegal means.[22] In this context data represents all personally identifiable information such as online cards details, name, telephone number, credit card number, social security number etc.[23]

In usual practice the State attorney can enforce this law and any institution that does not comply with the same can be legally prosecuted. It is vital to note that any such organization that provides data breach information notice to New York resident should also notify such information to the State Attorney, department of state and the police. In case it's there is a large volume of data which is breached and more than five thousand residents inhabiting in New York need to be notified, in that case such information of data breach should also be supplied to consumer reporting agencies with full details regarding the breach.[24]

2) Social Security Number Protection Law

Under this law, institutions are prevented from disclosing the social security number to anyone publicly. It includes and is not limited to mere printing of the social security number on any cards but also to retrieve other information. It also prohibits, sharing the social security number of individuals over the internet and printing and mailing it to the individual.[25] The social security number is very confidential and is issued by the federal government to the individual. The State Attorney General can enforce this particular law, and there is no private cause of action.

[22] N.Y. Gen. Bus. Law § 899-aa, available on www.codes.findlaw.com
[23] N.Y. Gen. Bus. Law §§ 899-aa(1)(a)-(b), available on www.codes.findlaw.com
[24] N.Y. Gen. Bus. Law §§ 899-aa(6)(a), available on www.codes.findlaw.com
[25] N.Y. Gen. Bus. Law §§ 399-dd(2)-(3), available on www.codes.findlaw.com

2.2.2) California Data Privacy Laws

Residents of California aptly recognized the need for strong data protection laws considering that technology companies are becoming quite vital in today's era. Data protection and enforcement of data privacy laws is an emerging area at the moment in government circles. California, with its advanced data protection laws has ensured that it is a step ahead of other jurisdictions. Therefore, entities complying with the data protection laws of California by default also ensure compliance with laws of other states regulating data protection. The jurisdiction of California covers Data Protection Laws as below -

1) California Financial Information Privacy Act

The California Financial Information Privacy Act (CFPIA) safeguards public interest by ensuring that corporates indulging in trade of selling personal non -public information without consumer permission are prosecuted.[26] Financial institutions and non-public personal information terms have the same definition as in the GLBA. This act can be enforced by the State attorney as no private cases are entertained.

According to this statute, companies need to take written consent, with signature and date from the customer in order to share any non-public personal information to the third party. The consent states that such customer is allowing full disclosure of his/her non-public personal information to third parties. In case the corporation wants to share such information to an affiliated party, it should annually communicate to the customer about such disclosure and notify them that they have not opted for any non-disclosure of the information.

[26] Cal. Fin. Code § 4052.5, available at. www.leginfo.ca.gov, 12th August 2014.

2) California Shine the Light Law

As per the California Shine the Light Law, any corporate that forwards personal information for marketing purposes to third parties, should disclose publicly its data sharing practices whenever any resident of the state asks them to furnish the same.[27] Institutions need to give a full list of the third parties with their contact information and also the notify kind of data shared to them. Institutions should set up a dedicated email address where residents can request such information.

Under this act personal information is defined as any information -- when it was disclosed, identified or described, was able to be associated with an individual. In this statute, personal information covers a wider scope to include information such as –

- Person's name and address or email id,
- Age or date of birth,
- height, weight, race, religion, occupation, political party affiliation,
- Children Details,
- Real estate transaction details,
- Banking card details (i.e., credit or debit card number),
- Investment account, debit or credit card balance.[28]

3) California Online Privacy Protection Act

The California Online Privacy Protection Act (Cal. COPPA) makes it mandatory for owners of website that are accessed by the general public (especially residents of California) and collect information from public need to prominently display their privacy policy on their website.[29] Personally Identifiable Information means the "information regarding a customer that can be individually traced and linked to that

[27] Cal. Civ. Code § 1798.83, *available at* www.leginfo.ca.gov, 20th April 2015.
[28] Cal. Civ. Code § 1798.83 (e)(7). available on www.codes.findlaw.com
[29] Cal. Bus. & Prof. Code § 22575(a), *available at* oag.ca.gov, 31st May 2015.

particular customer and is collected by an online website". The definition extends to data fields such as contact information, first and last name, social security number etc. and any other information collected by the website.

The entities that deal with the accumulation and maintenance of data need to comply with the privacy policy of the Cal .COPPA. It must be accordingly to the following provisions:

(i) The types of information collected needs to be marked.

(ii) Any third party with which the operator is sharing any kind of personal information needs to be shared.

(iii) Customers should be aware of the process to change any personal information if required.

(iv) The date of the privacy policy should be clearly stated.[30]

The organization should analyze their activities to determine whether it comply with Cal. COPPA, as when such organization's activity involves California resident then such organization are liable under Cal. COPPA. In recent times many instances have come up where the State of California Attorney General (CA AG) has questioned corporates involved in making mobile applications, on the failure to include any privacy policy.

4) District Of Columbia Data Privacy Laws

The Consumer Personal Information Security Breach Notification Act is a statute which has been enforced upon by the District of Columbia and it requires all corporates owning electronic data in its region to notify consumers in case any data breach has taken place.[31] If the numbers of people that need to be informed are more than thousand then they are also required by law to report the incident to the consumer reporting

[30] Cal. Bus. & Prof. Code § 22575(b), *available at* oag.ca.gov, 31st May 2015.

[31] D.C. Code §§ 28-3851 – 28-3853, available at www.beta.code.dccouncil.us

agency. Prosecution under this law may be initiated by private citizens or alternatively the attorney general.

Under this statute personal information comprises of the citizen's name, address, telephone number, social security number, bank cards number, bank account number, identification number issues by the District of Colombia etc.

2.2.3 Massachusetts Data Privacy Laws

The state of Massachusetts law undertaking practical approach enforces very minimal compliance requirements as far as data protection is concerned upon corporations, association, partnership or other legal entity and persons that maintain personal information of its residents.[32] Any institution which has sensitive personal data regarding Massachusetts residents must incorporate the Information Security Program which is included in the Massachusetts Data Privacy Laws. Personal information comprises of the resident's name, social security number, driver license, bank account number and identification number issued by the state to the citizen.[33]

In accordance with the Massachusetts Data Privacy Laws all corporates need to assess the data privacy risks and accordingly develop their security policy and ensure that it is strictly monitored to spot. The state requires that there should be an employee who looks after the maintenance of the security program. The policy should be reviewed annually and beyond that any deviations from the policy in practice should be identified and penalized accordingly.[34]

[32] 201 CMR § 1700 (2010), *available at* www.mass.gov, 9th January 2017.
[33] 201 CMR § 1702 *available at* www.mass.gov, 9th January 2017.
[34] 201 CMR § 1703 *available at* www.mass.gov, 9th January 2017.

2.3 OTHER STATUTORY FRAMEWORKS FOR DATA PROTECTION

Beyond the federal and state laws discussed, there are other equally vital statutes of this field which are:

2.3.1) Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) gives policies regarding credit card information. With digital payments becoming a critical factor in both developed and developing economies, the need for corporates to adopt to this technological shift is quite critical. This makes the policies surrounding online payments more relevant than ever. PCI DSS was formulated keeping in mind the protection of consumers. These policies need to be applied by corporates that gather, store, process or use cardholder data in their business operations. Some of the policies are-

- Companies should incorporate a firewall to safeguard such sensitive data.
- Corporates should reset all passwords for their equipment. They should not continue using passwords set by their suppliers. As there could be a breach of data.
- They should protect the cardholder data always.
- Any data which gets transmitted should duly be encrypted across the span of all networks.
- Anti-virus software needs to be updated to the latest version available.
- Systems that are maintained need to be secure and so do any applications that are interacting with the systems at any level.
- Cardholder data should not be accessible by all.
- Each employee should have a unique ID to identify him/her in case of any breach done by them.

- Anyone accessing cardholder data needs to be monitored and the data being accessed by them should also be checked if it's strictly for business use.
- Review network access privileges periodically.
- All systems need to be tested regularly for any issues.
- Policy should keep in mind information security for all employees.

2.3.2) U.S. EU Safe Harbor Framework

The European Union and U. S's Department of Commerce have collaborated to create a "Safe Harbour" framework, in which US companies can acknowledge themselves that they are compliant with EU laws for data protection. Companies that become a part of this initiative can easily transfer data between themselves. As of now there are twenty seven Member States of EU that are part of the initiative. The list of companies that are part of this initiative is displayed on the Safe Harbor Website so both EU and US. Organizations can see the companies in other countries before transferring any kind of data which is of a personal nature. Organisations are free to join the Safe Harbour Initiative as and when they wish to. The Safe Harbour Initiative in the US comes under the purview of the FTC as part of the FTCA which is there to prevent any misleading practices by companies. As part of the Safe Harbour initiative, any claims raised by citizens of EU against U.S, companies will be heard in U.S.

The Safe Harbour Initiative mandates that companies should comply with the following core principles –

- Notice- Companies should clearly tell individuals as to why their data is being collected, how will it be used by the companies and also how will it be protected. Companies should also give information as to how the grievance redressal mechanism would work for the consumers.
- Choice- Companies should give individuals choice to opt -in or opt-out of any data (with more protection to sensitive personal data) transfer to third parties where their data is going to be used for other uses than originally meant to be used.

- Onward Transfer: All third parties that are working in conjunction with them also need to comply with Safe Harbour data practices.
- Access: Individuals should duly be given access to change their personal information if the costs for doing so is not high and it does not in any way interfere with any other individual's rights.
- Security- Corporates need to ensure they have implemented a host of security measures to prevent any data breach by loss, theft etc.
- Data Integrity – It is vital that all sensitive personal information is used for the correct purposes only and no other reason.
- Enforcement- Organizations should ensure that they have a proper grievance redressal system and there should be identified employees who are responsible for compliance with the Safe Harbour rules.

Companies that are part of this initiative need to ensure that their own privacy policies cover the seven Safe Harbour rules.

2.3.3) Cross-Border Privacy Rules System (US-APEC)

The US became a part of the Cross-Border Privacy Rules System (CBPR System) in the year 2012. The CBPR was originally formulated by Asia-Pacific Economic Cooperation (APEC) under which organizations agree to comply with a host of standard policies governing data protection, thereby giving them the right to transfer data between countries. The policies under this need to be approved by an authorized APEC Accountability Agent who testified as to what degree is the company compliant with the CBPR guidelines. Once a company is certified and its privacy policies are agreed upon, they can freely be enforced by defined authority upon the company. The CBPR fundamentally contains four key statutes-

- Self-assessment: Organizations can use the APEC approved questionnaire which is duly furnished by the APEC-Accountability Agent. The questionnaire seeks basic

details such as notice, collection limitations, uses of personal data, choice options, security procedures, data access along with corrections, redressal systems etc.

- Compliance Review- The questionnaire is duly submitted to the Accountability Agent, for review. They then perform check to ascertain if the compliance procedures are implemented in accordance with the CBPR requirements.
- Recognition/Acceptance:-Organizations compliant with the CBPR are listed publicly in a directory, this allows customers to know. Besides the enforcement agent for each company where they can seek any complaint resolution as well as the agents who approved their compliance are listed.
- Dispute resolution and enforcement: The Accountability Agents and Privacy Enforcements Authorities can enforce the CBPR compliance in the companies they assess.

Since this is a very critical topic, the U.S. government is quite active in this field since 2013-

- It prosecuted advertisers for taking geo location and device identification numbers from a company giving free torch mobile application. The company took data without taking the user's consent.
- It also charged medical billing corporates for not safeguarding data of clients. This security lapse could lead to unauthorized leakage of customer's health related data.
- It charged companies that misled people stating that their privacy policies were in compliance with the Safe Harbour initiative.
- It prosecuted companies manufacturing internet cameras as they failed to safeguard customer privacy. Anyone with internet address of the device could view live footage.

3. DATA PROTECTION LAWS IN EUROPEAN UNION

EU law is an amalgamation of treaties and ancillary EU laws. The treaties such as the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU) are ratified by all EU member States and are thereby called 'primary EU

law'. The institutions that have been approved and given legal authority by the EU are thereby called "EU secondary law".

3.1 BACKGROUND

The Council of Europe was formed during the outbreak of the Second World War with a primary aim of unite all European states and promote democracy, social progress, law and fundamental human rights. In 1950, Europe adopted the European Convention on Human Rights (ECHR). It came into effect in 1953. All States need to follow the statutes laid down by the EHCR. The member states of COE made their national law in consonance with the ECHR, which obliged them to act in harmony with the provisions of the Convention. To make sure that the Contracting Parties observe their obligations under the ECHR, the European Court of Human Rights (ECtHR), was established at Strasbourg, France, in 1959. Safeguarding of personal data comes under Article 8 of EHCR which fundamentally gives citizens the right to respect of domestic life and communication and it also gives guidance on the circumstances under which restrictions of this right is permitted.

With passage of time the ECHR has examined various ancillary grey areas surrounding data protection such as surveillance and safeguarding confidential personal data from government agencies. However the ECHR has clarified in Article 8 that it prohibits any member nations to prevent any actions that breach their core principles, that of giving due respect to private and family life.

Since the information technology field has grown by leaps and bounds, it has become of paramount importance to formulate detailed rules and procedures to safeguard rules. In the 1970s various clauses regarding the protection of confidential personal data were adopted by the Committee of Ministers of the Council of Europe.[35] Convention 180 was adopted in 1981 which dealt primarily with the processing of data

[35] CoE, Committee of Ministers (1973), Resolution (73) 22 on the protection of the privacy of individuals *vis-à-vis* electronic data banks in the private sector, 26 September 1973, available at www.wcd.coe.int.

without human intervention was opened for signature.[36] Convention 108 still remains, the only legally binding international instrument in the data protection field.

The Convention 108 is universal in nature and is compiled by private and public bodies. It also gives protection against individual's data abuses during the data flow between countries. The convention provides reliability on the general accumulation and processing of personal data along with proper legal safeguards for the processing of 'sensitive' data. Although the convention provides for free flow of personal data between State Parties, it imposes some regulation on the data flow between government bodies. The EU was formally declared as a party to the Convention held in 1999. [37] In 2001, there were additional clauses that were added to it. These dealt with data flow between member countries and non-member countries. In such a case data flow would be allowed provided the non -member countries have an established data protection body which governs data flow.

Directive 95/46/EC is the chief legal instrument of European Parliament and the Council. It was established on 24 October 1995 and dealt with primarily safeguarding private data and the transmission of data (*Data Protection Directive*).[38] It was enacted in 1995, when most Member States already had established some regulation revolving around the matter of data protection. It was agreed that free flow of data, capital and manpower was not possible between member States unless they had a uniform data protection regulation between all States.

[36] CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, CETS No. 108, 1981, available at www.wcd.coe.int.

[37] CoE, Amendments to the Convention for the protection of individuals with regard to automatic processing of Personal Data allowing the European Communities to accede, adopted by the Committee of Ministers, in Strasbourg, on 15 June 1999; Art. 23 (2) of the Convention 108 in its amended form, available at www.wcd.coe.int.

[38] Data Protection Directive, Official Journal of European Communities 1995 No. L 281/31, available at ec.europe.eu.

The core belief behind the Data Protection Directive was to ensure that national law in member states is fairly uniform so that there is less confusion of legal interpretation. The Data Protection Directive fundamentally aims to provide same level of rights to all citizens in member states as far as the protection of private rights to individuals is concerned. The design of Data Protection Directive gives meaning to the right to privacy which is already contained in Convention 108 and it further expand them. The Data Protection Directive can in accordance with Article 11 of the Convention 108, make any changes to privacy rights. This kind of system creates a parallel form of supervision over existing law and thus ensures that the law is quite competent enough to meet the challenges of data protection. The Data Protection Directive is not limited to the 28 EU Member States only but it also covers non-EU member states such as Iceland, Liechtenstein and Norway which form a part of the European Economic Area (EEA).[39]

3.2 CONCEPT OF PERSONAL DATA AND OTHER RELATED TERMS UNDER DATA PROTECTION DIRECTIVE

As per EU data protection law and the CoE law, 'personal data' comprises primarily of information through which one can come to know, as to which person is the data referring to. The individual in this case is referred to as the 'data subject'.

3.2.1. Concept Of A Person

People form the core of data protection. Respect for private life is the baseline of the data protection law. The ECtHR's regulations in terms of Article 8 point out that sometimes it becomes very difficult for people to pick out personal and professional life individually as both lives get merged.[40] For example in the case of Amann v.

[39] Agreement on the European Economic Area, OJ 1994 L 1, which entered into force on 1 January 1994, available at ec.europe.eu.
[40] ECtHR, Niemietz v. Germany, 13710/88, 16 December 1992, available at www.worldlii.org.

Switzerland,[41] it was observed that the government body chose to record a business phone call of the party and on the basis of that information, further legal action was taken by the State. The ECtHR interpreted this as a clear violation of the person's private life and storing of such data was thus deemed illegal. It stresses upon the fact that forming relationships with other people comes under the ambit of 'private life', furthermore, there was no reason of principle to justify excluding activities of a professional or business nature from the notion of 'private life' and hence it was considered as a clear breach of Article 8 of ECHR.

This also brings us to the question as to why this data protection should only include natural persons and not seek to cover other things too. The EU data protection law only puts its focus on the natural persons. The law in place does not seek to include other legal persons such as corporates which are regarded as an artificial legal person against the use of their data under Article 8 of the ECHR. The Court, however, examined the case under the right to respect for home and correspondence, rather than under private life. Hence, according to Convention 108, data protection deals, primarily, with the protection of natural persons; however, the contracting parties may extend data protection to legal persons in their domestic law. However, EU data protection law does not, in general, cover the protection of legal persons with regard to the data processing that concerns them. The EU data protection law leaves it to legislators at a national level to decide the treatment of data protection in relation to artificial legal persons.[42]

3.2.2. Concept Of Identifiable Person

Both EU data protection law and CoE law, information incorporates data about a person only if the below parameters is met.:

- A particular person is explicitly identified in this information; or

[41] ECtHR, Amann v. Switzerland [GC], No. 27798/95, 16 February 2000, para. 65, available at swarb.co.uk.
[42] Data Protection Directive, Recital 24, available at googleweblight.com

- If an individual who is not identified but adequate data is disclosed wherein after some basic research one would be able to identify him/her.

The above information is legally protected as per the data protection law. The ECtHR has repeatedly stated that the concept of 'personal data' under the ECHR is the same as in Convention 108, specially relating to the condition of identifiability of an individual.[43] Moreover identification needs basics which describe a person in such a way that he or she is distinguishable from all other persons and recognizable as an individual. Name for an example of a person cannot by itself be called an identifier as there are many people with similar names. Hence more identifiers are needed to accurately recognize a person and not confuse him/her with anyone else. Date and birthplace are used as the common identifiers to verify a person's identity. In addition, personalized numbers have been introduced in some countries for better recognition of their citizens.

However in many places, new age technology is used such as biometrics, iris scans etc. to accurately recognize people. In the European data protection law, there is no mandate for ensuring advanced recognition techniques. A person is regarded identifiable if a piece of information contains essentials of identification through which the person can be identified, whether directly or indirectly.[44] In accordance with the Recital 26 of the Data Protection Directive, the primary basis is whether it is likely that reasonable means for identification will be accessible and administered by the target users of the information. This clause also includes third-party.

3.2.3. Concept Of Personal Data

Any type of information that concerns an individual is personal data. Personal data covers specific information of an individual's personal and professional life. It may be noted that the link between a person and an event can both qualify as personal data

[43] ECtHR, Amann v. Switzerland [GC], No. 27798/95, 16 February 2000, available at swarb.co.uk.
[44] Data Protection Directive, Art. 2 (a), available at www.dataprotection.ie.

eg mobile phone of a particular person getting lost. It is important to note that while safeguards are necessary, however the data protection law does not specify the form in which any data is supposed to be stored. Personal data can be textual or visual and also sound at times,[45] Eg written text, camera recordings (CCTV) or recorded call.[46] It is observed that even cell samples are likely to be treated as personal data as they do incorporate the DNA of a person.

3.2.4. Concept Of Sensitive Personal Data

As far as the EU data protection act is concerned, there are specific data which pose massive risk to its subjects and therefore it needs more special treatment at the time of processing it. These special categories of personal data are known as Sensitive Personal Data and the processing of such sensitive personal data must therefore be allowed only with specific safeguards. Both the Convention 108 (Article 6) and the Data Protection Directive are unanimous on personal data related to below points-

- race or ethnic origin;
- political opinions, religious or other beliefs;
- health.[47]

The Data Protection Directive also emphasizes on 'trade union membership' as it correlates to political belief of a person. In accordance with Article 8 (7) of the Data Protection Directive makes obligatory for EU member States "to determine the fundamental conditions under which a national identification number or any other such data will be processed."

[45] ECtHR, Von Hannover v. Germany, No. 59320/00, 24 June 2004; ECtHR, Sciacca v. Italy, No. 50774/99, 11 January 2005, available at www.5rb.com>Cases
[46] ECtHR, Peck v. the United Kingdom, No. 44647/98, 28 January 2003; ECtHR, Köpke v. Germany, No. 420/07, 5 October 2010, available at www.5rb.com>Cases
[47] Article 8 of the Data Protection Directives, available at www.dataprotection.ie.

3.2.5. Concept Of Anonymised and Pseudonymised Data

Data will inherently become anonymised if all particular identifiers are removed. In such cases one would need to put in substantial effort in order to identify the particular person.[48] If personal data is completely anonymized then it becomes irrelevant, and storage of such anonymized data in a personalized form for the purpose of historical, statistical or scientific use are allowed under Data Protection Directives.[49]

Personal information contains identifiers, after getting pseudonymized the identifiers are replaced with only one particular pseudonym. There is no clear mention of Pseudonymised data in the definitions given in either Convention 108 or the Data Protection Directive. However, the Explanatory Report to Convention 108 mentions in Article 42 that while the data need not be separated permanently from the person's name, there should always be a provision to relink and establish suitable linkage between the identifiers and the related data. This is an effect which can be achieved by pseudonymising the data.

3.2.6. PERCEPTION OF DATA PROCESSING

The Data Protection Directive mainly revolves around the regulations of automatic data processing. As per the EU law, automated data processing refers to the process where any data is processed completely or in certain parts with non-human intervention.[50] According to EU laws Data Protection in no ways can stick only to automated data processing. Data protection in this aspect has a broadened view and also covers data which is stored in manual files for future retrieval. This is done for the following reasons-

- Manual filing makes it easy to organize data based on some parameters; and

[48] Data Protection Directives, Recital 26, available at googleweblight.com.

[49] Data Protection Directive, Art. 6 (1) (e), available at www.dataprotection.ie.

[50] Data Protection Directive, Art. 2 (b) and Art. 3 (1), available at www.dataprotection.ie.

- Storing data in physical files might be used as a turnaround to sabotage the principles of the data protection directive.[51]

It is important to observe that data processing is a fairly comprehensive concept and this means that act done or series of ancillary acts for storing, collecting, recording, organising, amending, retrieval, consulting, using, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction etc. on personal data , comes under its purview.[52] Even processing qualifies as a mere transfer of responsibility from one controller to another controller in the usual course of business.

3.2.7. USERS OF PERSONAL DATA

The key components of personal data are: Data Controllers, Data Processors, Data Recipients and Third Parties.

1) Data Controller

As per the clauses of the EU data protection law, a controller is mainly someone who independently or in conjunction with other decides the purpose and process of data processing.[53] Hence, the controller has overall discretion, on how data will get processed and moreover what different types of raw data will be stored and for how long. Data controllers are identifiable and are personally responsible in case there is any data processing that happens illegally. A request for deletion must therefore always be addressed to the 'factual' controller.

The term 'controller' as per the Data Protection Directive can also be interpreted as a group of companies that are jointly managing data control. The law does not

[51] Data Protection Directives, Rectical 27, available at googleweblight.com.
[52] Data Protection Directive, Art. 2 (b), available at www.dataprotection.ie.
[53] Data Protection Directive, Art. 2 (d), available at www.dataprotection.ie.

indicate that the purpose of data control of all entities that are jointly managing it be the same.[54] This is legally possible, excluding certain cases where a special legal basis provides for processing the data jointly for a common purpose. This is a grey area subject to further legal interpretation. The entities may have common or diverse purposes.

2) Data Processor

Under EU data protection a data processor is basically someone who works under the controller to process the data under supervision.[55] Processors may be given diverse range of activities surrounding data protection. Such processors are in turn also data controllers in their own authority for the work they are given to perform.

3) The Third Party

The term 'third party' is someone who is distinct from the controller. There should be a bonafide reason for any data transfer to third parties. As per the Article 2 (f) of the Data Protection Directive, a third party refers to any individual, corporate, public authority or any other body that is not the main data subject, or the data controller and/or processor. This can be interpreted since their legal constitution differs, from the main head company even if they are part of the same group. Bank branches processing customer's accounts under the direct authority of their headquarters would not be considered as 'third parties'[56].

a. Data Recipients

'Recipient' is more comprehensive than 'third party'. As per Article 2 (g) of the Data Protection Directive, recipient could be any individual, agency, public authority, corporate or any other body with whom data is shared. The recipient can be person

[54] Data Protection Directive, Art. 2 (d), available at www.dataprotection.ie.
[55] Data Protection Directive, Art. 2 (e), available at www.dataprotection.ie.
[56] Article 29 Working Party (2010), Opinion 1/2010 on the concept of 'controller' and 'processor', WP 169, Brussels, 16 February 2010, p. 31, available at ec.europe.eu.

outside the controller or processor – this would then be a third party – or someone inside the controller or processor, such as an employee or another division within the same company or authority.

As per structure the controller is considered to be the driving force behind data protection and its methods use. Controller however is responsible for the processing done by the data processors. The controller must manage compliance of the data processing function in accordance with applicable laws. So it may be interpreted that any binding contract that forbids the controller to make decisions of processing will result in dual controllership, thereby absolving the controller from legal responsibility.

The legal distinction between the recipient and third parties is critical. While recipients may be the data processors or controller along with the employees of controller themselves as they receive data to process it. However, any data possessed by a third party should have a legal reason for it; absence of it would declare it as an illegal possession of confidential data. 'Third-party recipients' of data will, therefore, always need a legal basis for lawfully receiving personal data.

3.2.8 PERCEPTION OF CONSENT

As per Article 2(h) of the Data Protection Directive consent is defined as "any free indication of the data subject's wishes." Consent is the core backbone behind data collection, processing or its subsequent storage anywhere. As per the EU data protection law, the following conditions are deemed necessary for anything to constitute as consent.

- The data subject should not be under any kind of external pressure while he/she is giving consent.
- It is important that the data subject has been informed of the ramifications of giving his/her consent, and
- The overall scope of consent given should be on reasonable grounds.

It is to be noted that both the European civil law and the Data Protection Directive have the same requirements for qualifying any consent. Beyond the rules mentioned above, there are also some fundamental legal laws that apply as far as consent is concerned. For people who do not have any legal basis, their consent will not count as legal basis for protecting data. The consent can be given either explicitly or non-explicitly.[57] Explicit consent is clear in its intentions and can be made either orally or in writing; while non-explicit consent concluded from the circumstances. Consent - should be specific in nature and not unambiguous. Consent can be free consent, informed consent and specific consent depending upon the circumstance under which the consent is acquired.

a) Free Consent

The concept of free consent is only of any value if the data subject can exercise an actual choice in and there lies no fear or threat if the subject does not give his /her consent.[58]. It may also happen that there is a natural imbalance between the data subject and controller in terms of economic power etc. which could lead to a forced consent. [59] Negative consequences of not consenting do not mean that the consent can never be valid; it majorly depends upon the circumstances prevailing while consenting or not consenting. There are situations wherein, lack of consent leads to undesired aspects in day to day life eg your local supermarket may not give you additional discount if you are unwilling to provide them your contact details. There are also situations wherein getting products or services are directly conditional upon disclosing data. In such situations it is fair to assume that the consent given is not on a fair basis.

b) Informed Consent

The data subject must have adequate information at his/her disposal before giving their consent. They should be clearly explained the consequences of giving or not giving any

[57] Data Protection Directive, Art. 8 (2), available at www.dataprotection.ie.
[58] Article 29 Working Party (2011), Opinion 15/2011 on the notion of consent, available at ec.europe.eu.
[59] Article 26 (1) of Directive 95/46/EC of 24 October 1995, available at www.dataprotection.ie.

consent and beyond that a clear description of why consent is being taken must be given. The language should be understandable to the data subject and should be in accordance with the location. There should be adequate accessibility as well as visibility of information. The data subject should be given a brief description and along with that the option to go in depth to seek more details of the case in case he/she wishes to do so.

c) Specific Consent

For consent to qualify as valid consent it is equally important that the consent given is specific in nature. This goes hand in hand with the quality of information given about the object of consent. In this background, the reasonable expectations of an average data subject will be relevant. The data subject must be asked again for consent if there is any change to data processing or any additional requirement that need to be changed if things were not known while giving initial consents.

d) Right For Withdrawal Of Consent

The Data Protection Directive does not categorically specify the right to withdraw any consent given. It would ideally be possible that a data subject might withdraw his/her earlier consent on some reasonable grounds. Having said that, there is no compulsion to state any reasons for withdrawing and beyond that no ancillary negative consequences for the same.

3.3 IDEOLOGIES OF THE DATA PROTECTION DIRECTIVES

In accordance with the Article 6 of the Data Protection Directive, all subsequent laws regarding data protection legislation in EU or CoE need to follow ideologies and keep in mind those before framing any subsequent laws. Any exceptions of the same

should duly be covered under national law. [60] The following ideologies need to be kept in mind for it-

3.3.1 Lawful Processing

Processing of personal data will duly be seen as interference to the personal life of data subject concerned. This right again is not absolute within itself and is balanced by public interest which are given due importance. As per the ECtHR, any such interference would be within limits of domestic laws. It is said that law should be accessible to all people and it should be a law which addresses foreseeable issues.[61] Generally speaking a rule is foreseeable if it is formulated with enough care to give an individual sufficient advice regarding to mind his/her behavior as a civic citizen.[62]

As per the ECtHR, any kind of undue interference is considered acceptable if it adequately addresses a particular social need and has the core purpose to protect the rights of other citizens.[63] Article 8 (2) of the ECHR states that lawful processing means that the conditions for justified interferences are the minimum requirements for the lawful limitations of the right to data protection according to the Charter. Legal processing of personal data mandates under EU law that the conditions of Article 8 (2) of the ECHR at least be fulfilled all the times; EU law could, however, state extra requirements for exceptions. The principle of lawful processing under EU law and the relevant provisions of the ECHR is further extended by Article 6 (3) of the TEU, provides that "fundamental rights, which are guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms, also form general principles of the Union's law".

[60] Data Protection Directive, Art. 13 (2), available at www.dataprotection.ie.
[61] ECtHR, Amann v. Switzerland [GC], No. 27798/95, 16 February 2000, para. 50, available at swarb.co.uk.
[62] ECtHR, Amann v. Switzerland [GC], No. 27798/95, 16 February 2000, para. 56, available at swarb.co.uk.
[63] ECtHR, Leander v. Sweden, No. 9248/81, 26 March 1987, para. 58, available at swarb.co.uk.

3.3.2 Specification and Limitation

The main principle of purpose specification and restriction means that the legal processing of personal data will depend mainly on the purpose.[64] The core purpose must have been stated and made obvious by the controller before starting the procedure of data processing. As per EU law, this should be done by explicit declaration, in other words by informing the appropriate supervisory authority or, at the least, by internal documentation given by the controller for inspection to the higher authorities. Every data processing request should be accompanied with a specific legitimate reason. In turn, legitimate processing is limited to its firstly specified purpose and any new purpose of processing will require a separate new legal basis. Disclosure of data to third parties will have to be considered carefully, as disclosure usually mandates a new purpose and therefore needs a legal basis, different from the one originally used for collecting the data.

So the processing of personal data for undefined and/or broad range of purposes is illegal. The Data Protection Directive states that the processing of data for historical, statistical or scientific is not considered as incompatible if Member States make sure that safeguards are in place. The Directives further provides that the compatible use of data can be allowed on the ground of legal basis. However, it may be noted the meaning of 'compatible' is not defined explicitly.

3.3.3.Data Quality

The type of data selected for processing must be necessary to achieve the declared overall aim of the processing operations, and a controller should restrict accumulation of only what is necessary for a specific purpose. Nowadays data relevancy has an additional consideration: by making explicit use of special privacy-enhancing technology, it sometimes is completely possible to avoid using personal data or alternatively use only pseudonymised data, which results in a privacy-friendly solution.

[64] Data Protection Directive, Art. 6 (1) (b).

A controller having personal information should ideally not use that information without taking steps to verify if the data is updated and correct. The obligation to ensure accuracy of data must be seen in the background of the purpose of data processing. There are cases where data accuracy and updating, is needed because of the undesirable ramifications to the data subject if data were inaccurate.

Article 6 (1) (e) of the Data Protection Directive mandates all Member States to ensure that personal data is kept so that subsequent identification and retrieval is done in accordance with the purpose for which the data was collected.[65] Such data should be wiped out once the original use is over. The time limitation for storing personal data applies, however, only to data kept in a form which permits identification of data subjects. If one wants to store unrequired data that is no longer needed one can keep it anonymised or pseudonymised. However storing data for potential scientific, historical or statistical use is explicitly exempt from the principle of limited data retention in the Data Protection Directive. Such ongoing storage and use of personal data must, however, be accompanied by special safeguards under national law.

3.3.4.Fair Processing

The principle of fair processing looks over the relationship between the controller and the data subject. This principle makes the controller responsible for establishing an obligation for the controller to keep data subjects informed on how data are used. It should be explained to the data subject in an easy to understand way.

Controllers should inform data subjects and public that their processing is done in a transparent way. Processing operations must not be performed in secret and should not have unforeseeable negative effects. Controllers should ensure that customers, clients or citizens are informed about the use of their data. Further, ccontrollers should always

[65] Data Protection Directive, Art. 6 (1) (c), available at www.dataprotection.ie.

work in accordance with the wishes of data subjects over matters regarding their data use.

With reference to internet services, data-processing system must be featured in such a way that it makes possible for data subjects to clearly understand about the use of their data. Fair processing also means that data controllers should go beyond legal requirements to keep data subjects informed.

3.4 RULES FOR DATA PROCESSING UNDER DATA PROTECTION DIRECTIVES

The Data Protection Directive contains different sets of procedures for lawful processing of data.

3.4.1.Lawful Processing Of Non-Sensitive Data

Chapter II of Directive 95/46, named as 'General rules on the lawfulness of the processing of personal data', states that barring exceptions permitted under Article 13, all processing of personal data must comply with the relevant principles provided under Article 6 concerning data quality and, secondly, with one of the criteria for making data processing legitimate, listed under Article 7.

Under EU data protection law, consent as a way for legal data processing is firmly stated in Article 7 (a) of the Data Protection Directive. Also Article 7 (b) of the Data Protection Directive provides different legal basis for data protection for such data processing and that it should only be necessary for the contract to get fulfilled.

According to Article 7 (c), of the Data Protection Directive, private controllers need to ensure that all their practices are completely in compliance with all local laws that they are subject to. Article 7 (e) of the Data Protection Directive covers mainly controllers that are present in public sector. The legal obligations of controller become

the foundation of lawful data processing. In many situations private controllers are obliged by law to process data of others; e.g. hospitals and doctors need to keep data on the treatment practices for patients for multiple years.

Article 7 (d) of the Data Protection Directive puts focus on the point that the processing personal data is legal if it is needed to protect the data subject's interests. Such data can be used for future analysis eg processing data of missing people would be considered as processing of personal information but it its very critical from a larger perspective. Even the fundamental rights protection should never endanger the crucial interests of the person who is protected.

Article 7 (e) of the Data Protection Directive explains that personal data can legally be processed if it is needed for the adequate performance of a public interest or to enforce of official power vested upon the controller or on a third party with whom the data are is shared". Article 7(f) of the Directive 95/46 states that in the absence of the data subject's consent, and to enable processing of that data subject's personal data as is necessary to practice in a genuine interests of the data controller or of the third party or, also inherently require that the fundamental rights and freedoms of the data subject be respected.

3.4.2.Lawful Processing Of Sensitive Data

Article 8 of the Data Protection Directive, mandates the practices needed for processing categories of data that reveal key demographics, political opinions, religious or philosophical beliefs, trade union membership or information on health etc. Processing of sensitive data is prohibited in general.[66] However, it may also be noted that a complete list of exemptions to this prohibition can be found in Article 8 (2) and (3) of the directive. These exemptions also involve direct consent of the data subject, crucial interest of data subject and genuine interest of the public at large. If sensitive

[66] Data Protection Directive, Art. 8 (1), available at www.dataprotection.ie.

data are to be processed as part of a contract with the data subject, use of these data requires the data subject's direct consent, and a statement agreeing for entering into the contract.

1) Clear Consent

The first condition for legal processing of any kind of data is the actual consent of the data subject. In the case of sensitive data, such consent must be direct and clear. National law states that a mere consent to use sensitive data does not justify the legal need for permitting data processing.[67] In one special case, even implicit consent is acknowledged as a legal basis for processing sensitive data: Article 8 (2) (e) of the directive states that processing such data is not banned and especially if data is made public by the data subject. According to the provision consent will be implied for the use of data when data subject is making his or her data public.

2) Interest of Data Subject

Sensitive data is crucially important for a data subject and hence it must be legally processed with extra safeguards.[68] In case where data subject cannot give his consent (i.e., data subject is unconscious, absent or could not be reached) for the processing of sensitive data, then it would be legitimate on the basis that it is to submit the question to the data subject for deciding.

3) Public's Genuine Interest

Article 8 (2) of the Data Protection Directive, provides provisions that if the genuine interest of others are involved then legal processing of sensitive data is valid but under following cases:

- where data subject is physically or legally incapable of giving his consent and his data processing is necessary because of the crucial interests of another person;

[67] Data Protection Directive, Art. 8 (2) (a), available at www.dataprotection.ie.
[68] Data Protection Directive, Art. 8 (2) (c), available at www.dataprotection.ie.

- where sensitive data are relevant in the field of employment law, such as health data, such as in the context of a specifically dangerous work place, or data on religious beliefs, such as in the context of holidays;
- where foundations, associations or other non-profit-seeking bodies with a political, philosophical, religious or trade union aim, process data about their members or sponsors or other interested parties (such data are sensitive because they are likely to reveal the religious or political beliefs of the individuals concerned);
- where sensitive data are used in the context of legal proceedings before a court or administrative authority for the establishment, exercise or defense of a legal claim.
- Moreover, according to Article 8 (3) of the Data Protection Directive where health data are used for medical examination and treatment by healthcare providers the management of these services is included in this exemption. As a special safeguard, persons are recognized as "health care providers" only if they are subject to specific professional obligations to confidentiality.[69]

Additionally, according to Article 8 (4) of the Data Protection Directive, Member States may introduce further purposes for which sensitive data may be processed, as long as:

- processing data is for reasons of large public interest; and
- it is provided for by national law or by decision of the supervisory authority; and
- the national law or decision of the supervisory authority contains the necessary safeguards in order to effectively protect the interests of the data subjects.[70]

[69] Data Protection Directive, Art. 8 (2) (c) – Art. 8 (2)(e), available at www.dataprotection.ie.
[70] Data Protection Directive, Art. 8 (4), available at www.dataprotection.ie.

3.4.3.Security Of Processing

The duty of controllers and processors is to put suitable measures in place to ensure data security is, therefore, is in accordance with what is laid down in EU data protection law. As per the required provisions in EU data protection law:

"Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network and against all other unlawful forms of processing."[71]

Secured processing of data has been governed, guided and developed by many industrial, national and international principles. The European Privacy Seal (EuroPriSe) is an eTEN (Trans-European Telecommunications Networks) project of the EU which has particularly navigated possibilities of certifying products, especially software, to being in compliance with European data protection law. The European Network and Information Security Agency (ENISA) were set up to enhance the EU member's states and business community to prevent, address and respond to network and information security hurdles. ENISA on a regular basis prints analysis of current security threats and advice on how to address them.

Data security is not just accumulated by the right equipment – hardware and software – in place. It needs to be governed by some principles such as-

- spreading awareness of obligations and confidentiality amongst the employees for data protection;
- proper distribution of roles & responsibilities for data processing with special reference to processing of personal data and transfer of data to third parties;
- usage of personal data should be in accordance to the competent person's instructions as well as in accordance to general rules;

[71] Data Protection Directive, Art. 17 (1), available at www.dataprotection.ie.

- restricting access to locations and to hardware- and software of the controller or processor.
- ensuring that authorizations to access personal data are granted by the competent person and with due documentation;
- automated protocols for access to personal data inbuilt in the system and regular random checks of such protocols by the internal supervisory desk;
- Full documentation for other kinds of disclosure than automated access to data in order to be able to demonstrate that no illegal data transmissions have taken place.

Granting sufficient and relevant data security education to the staff members is also a critical element of effective security precautions. Verification procedures must also be inbuilt in order to make sure that these measures not only exist on paper but are also implemented. Personal data protection officials, security education to the employees, steady audits, penetration tests and quality seals are some of the instruments which help improving the security level of a controller or processor.

1) Confidentiality

Under EU data protection law, the secure processing of data is further protected by the general duty of all persons, controllers or processors, to be sure that data remain confidential. Article 16 of the Data Protection Directive revolves around confidentiality only within a controller– processor relationship. The controllers are mandated to keep data confidential, in a way that they may not disclose them to third parties, which is compliant with Articles 7 and 8 of the directive. Confidentiality does not cover situations where data is known to a person in his or her capacity as a private individual and not as an employee of a controller or processor. Article 16 of the Data Protection Directive does not apply to this case at all, as, in fact; the use of personal data by private individuals is totally exempted from the directive's remit where such use falls within the margins of the so-called household exemption.

Processors need to follow instructions given by controller all the time. For the employees of a controller/processor, confidentiality implies that they use personal data only according to the instructions given by their superiors. Duty of confidentiality must be on contractual basis between controller and their processors. Additionally employment contract contains clauses of confidentiality which lays legal duty over the employees of the controller and processors.

3.4.4.Transparency Of Processing

The principle of fair processing requires transparency in processing. EU data protection law is quite specific, for securing transparency on behalf of the data subject by levying duty over the controller to inform the data subject, and for the general public through notification. Further EU data protection law states that, exemptions and restrictions from the transparency implementation by the controller may exist in national law when such a restriction constitutes a necessary measure to safeguard certain public interests or the protection of the data subject or of the rights and freedoms of others, as long as this is necessary in a democratic society.[72]

1) Ways of providing information

The ideal way of providing information would be to inform every single data subject, orally or in writing. Both data accumulation and giving information should go hand in hand. In case where data is collected from third party data subject should be reached through the way of appropriate publication (where data subject could not be reached personally due to practical difficulties). One of the most effective ways to provide information will be to display information clauses on the home page of the controller, such as a website privacy policy. While using the above way it should be also be taken into consideration that majority of the population does not use internet and therefore providing the information of company's policy or public authority ought to be taken in account.

[72] Data Protection Directive, Art. 13 (1) , available at www.dataprotection.ie.

2) Information

According to EU data protection law, controllers of processing operations are duty bound to inform the data subject in advance about their intended processing practices. The said duty of controller is not dependent on the request from data subject. This duty does not depend on a request from the data subject but it must be given proactively by the controller, despite of whether the data subject shows interest in the information or not. The information must encapsulate the purpose of processing, and details like identity and contact number of the controller.[73] Additional information is to be given where it is necessary in specific circumstances in which data are accumulated to guarantee fair processing of data in compliance with the Data Protection Directive. Articles 10 and 11 of the directive frameworks, the categories of data processed and the recipients of such data along with the information about the core right to access and amend. Where data are collected from the data subjects, the information should clarify whether replies to the questions are mandatory or not, as well as the possible consequences of a failure to reply.[74]

Fair processing requires information be easily understandable by the data subjects. Language must be used which is appropriate for the addressees according to the local language. Some data people will want to be informed only in a brief manner as to how and why their data is being processed, whereas others will require a comprehensive explanation. Article 11 (2) of the Data Protection Directive states that data subjects need not be informed about processing operations if they are laid down by law.

3) Notification

As per EU data protection law, controllers can choose to appoint a personal data protection official, who is liable in particular for keeping a record of processing operations carried out by the controller. This internal record must be made available to members of the public on request in a transparent manner. The publication of

[73] Data Protection Directive, Art. 10 (a) and (b), available at www.dataprotection.ie.
[74] Data Protection Directive, Art. 10 (c), available at www.dataprotection.ie.

notifications by the supervisory authority must be in the form of a special register. In order to accomplish its purpose, access to this register should be given for free and in easy manner. Article 18(2) lists the clauses for exemptions from the duties to notify competent supervisory authority or to appoint internal data protection official which might cause specific risk to the data subjects.

3.4.5.Encouraging Compliance

Developing accountability, the Data Protection Directive mentions several instruments for encouraging it:

1) Prior checking

Article 20 states that due diligence should be done by the supervisory authority to safeguard specific risks posed against the rights and freedoms of the data subjects before even beginning the data processing. A supervising authority should ensure that this check is done before commencing data processing. The supervisory authority is empowered to take coercive actions and even fine the controllers for not executing their duty of notification.

2) Personal data protection officials

The Data Protection Directive allows controllers to appoint a person specifically as a personal data protection official. This is done in the best interests to safeguard the rights and freedoms of data subjects. To do things accurately one will need to give some independence to such an official as he/she does their duty. Efficient functioning of this office depends on strong employment rights to guard against eventualities such as unjustified dismissal would also be necessary.

3) Codes of conduct

To ensure proper compliance the best practices and the processing activities can be made into a rule manual. This will help corporates to look at it whenever they face any

doubt on their own practices. The European Commission encourages having a code of conduct specific to the sector, so it can help in proper implementation of the data practices.[75] Data Protection Directive, Member States also need to formulate a standard procedure for evaluating the Code of Conduct framed. The above said procedure would require the national authority involvement along with the support of trade associations and other bodies representing categories of controllers.[76]

3.5 RIGHTS OF DATA SUBJECT

Every data subject should be given rights to question controller if his/her data is being processed. Thus, national law grants them the following-

- access their personal data by asking the controller who has their data for processing;
- have their data amended in case the data controller has incorrect data;
- get their data deleted or blocked in case it is found that the data has been illegally obtained for processing by the controller;
- to raise questions about the data processing if it has undesirable consequences;
- to object in case their own data is being used by marketing companies.

3.5.1 Right of access

The Article 12 of Data Protection Directive states that certain provisions such as the right to access along with the right to obtain confirmation from the controller about their data being processed or not, purpose of processing of data, categories of data concerned and recipients to whom the data is disclosed. Also, the data subject has right to obtain information like rectification, cancellation or blocking of data processing that does not comply thoroughly with the Data Protection Directive.

[75] Data Protection Directive, Art. 27 (1) , available at www.dataprotection.ie.
[76] Data Protection Directive, Art. 27 (2) , available at www.dataprotection.ie.

As per Article 13 of the Data Protection Directive there may be some contradictory legal interests of others as a result of which the data controller may be unable to accept the data subject's request for his/her data. Superseding legal interests can be various types such as national security, public security, prosecuting of criminal offences and also sometimes private interests where the interest of data subject subsides. The Data Protection Directive allows processing of data for scientific research of statistical purposes with narrowly applicable access rights by the national law; however, safeguards need to be in place at all times. Article 13(2) of the Data Protection Directive mandates that no decisions are taken regarding the data subject on the basis of data processing and at no point should the data subject's privacy be breached.[77]

3.5.2 Right to Access One's Own Data

Right to access one's own data is the right provided under in Article 12 of the Data Protection Directive. Data subject should have full access and knowledge about his data being used and even the data currently in process by the data controller. Controller is duty bound to explain the data subject in details about what category of data is to be processed. Information about source of data which is processed must be given to the data subject by the controller. Data subject can also get information as to what category of data is being used and also to whom is it going to be distributed. In case data is being processed by way of computers without human intervention the data subject must be explained logic being used to process this data.

3.5.3 Right to rectification, erasure and blocking of data

As per the Data Protection Directives Recital 41, all data subjects have a right to ask for any changes or also blocking of their data if they feel that data processing is not done in accordance to the data protection directive.[78] Precisely this provision provides the data subject with the right for rectification, erasure and blocking of his own data.[79] In certain

[77] Data Protection Directive, Art. 13 (2) , available at www.dataprotection.ie.
[78] Data Protection Directive, Recital 41, available at googleweblight.com.
[79] Data Protection Directive, Article 12(b) , available at www.dataprotection.ie.

cases, if the rectification relates to spelling mistake or change of address a simple request for rectification would be sufficient for the controller for making changes. However, in some cases where there is a link to legal issues it may be possible that the data controller may ask for proof of inaccuracy from the data subject if needed.

Data subjects usually request erasing of data when they suspect that data processing is not done legitimately. This situation arises in the case where the original consent is withdrawn or maybe data becomes irrelevant to the original purpose of data collection. As per the provision controller at all the time should have a rationale to defend the data processing taking place. The data subject can object to the data processing and can demand that the data be blocked till further investigations reach to a conclusion. With this the data controller will not be able to use the data. National law should give more clarity on this provision to advise when and how it can be used .It may be observed that inaccurate data may even cause harm to the data subject.

It is important that in case there is any rectification done in data or it is required to be erased then all parties to whom it is disclosed need to be contacted and advised of it unless it is impossible to reach out to so many parties. Contacting data recipients for the rectification, deletion or blocking of data is mandatory, "unless this proves impossible or involves a disproportionate effort" as per the provisions of Data Protection Directives.[80]

3.5.4 Right to object to automated individual decisions

Data subject have a right to contest to any automatic decisions that take place regarding personal data. Such decisions taken by automatic means on the basis of inaccurate data can harm the data subject leading to undesirable consequences. If such decisions are likely to have considerable impact on the lives of individuals as they relate, for instance, to creditworthiness, performance at work, conduct or reliability, special protection is

[80] Data Protection Directive, Art.12 (c), available at www.dataprotection.ie.

necessary to avoid inappropriate consequences. The directive mandates that the individual be given rights to review the automatic decision affecting him/her.[81] Member states need to ensure that since data in question concerns the data subject so adequate provisions need to be kept in place.[82]

3.5.5 Right to Object about the processing of their data if it leads to disproportionate results.

There is no general right of data subjects to object to the processing of their data. There is a provision under Article 14 (a) of the Data Protection Directive wherein a data subject may object to a situation that leads to undesired consequences. Such provisions aim at finding the correct balance between the data subject's data protection rights and the legitimate rights of others in processing the data subject's data. If such right is exercised then the data controller has no authority to continue processing the data. However if such data is already processed before the data subject protested, then the data processes still remains legal.

3.5.6 Right to object to further use of data for direct marketing purposes

According to Article 14(b) of the Directive, the data subject may have right to object for their data given out for direct marketing purposes. Similar rights are also discussed in the CoE Direct Marketing Recommendations. This right can be exercised before data is disclosed to third party marketing companies. Hence, the data subject must be given the opportunity to exercise his right to object before the data are transferred for marketing purpose.

3.5.7 Independent Supervision

The Data Protection Directive mandates there should be an independent supervising body that would effectively ensure that data protection is complied in the right manner.

[81] Data Protection Directive, Art.15 (1), available at www.dataprotection.ie.
[82] Data Protection Directive, Art.15 (2), available at www.dataprotection.ie.

The directive introduced an instrument for the enforcement of data protection which did not appear, at first, in Convention 108 or in the OECD Privacy Guidelines. Independent supervision is critical for data protection as it ensures that there are no lapses and holds the responsible people accountable for any deficiencies in data protection measures taken. OECD privacy Guidelines revised edition of 2013 added new provisions which states that the Member states should empower the supervision bodies with adequate resources and power in order to do their work properly and ensure that it is done in an impartial manner at all times.[83] The outline of competence and organizational structure of supervisory authorities was for the first time described under Article 28 (1) of the Directive. Data Protection Directive requires Member States to give complete independence to be given to the authorities to execute their duties.

The supervisory authorities have powers to guide data controller and data subjects on all the matters, to ensure that they are following the best practices to safeguard the data, to investigate and intervene in the data processing operations, to warn the controllers, to order rectification, blocking, deleting and destruction of data, to order for temporary or definitive ban on processing and to refer the matter to court. During the course of an enquiry the supervising body should have full access to personal data so they can investigate and take any required action. Supervisory authorities are also empowered to ban or restrain data controllers from processing data if they feel that it is being done in a manner which is not in the best interests of the data subject.

3.6 REMEDIES AND SANCTIONS

As per the Data Protection Directive the national laws in place should adequately address any breaches of the data protection act. Only the data subject whose personal rights are endangered may exercise it. Children need to be represented by their

[83] OECD (2013), *Guidelines governing the protection of privacy and transborder flows of personal data*, para. 19 (c).

guardians in such cases. It is also possible that people from associations which seek transparency and advocate data protection rights may have their member testify in court.

3.6.1 Requests to the controller

In most cases one should address all matters of concern to the data controller itself. In case one is not satisfied with the response, one may move to higher judicial authorities for suitable remedies. As per the Data Protection Directive, provisions under Article 12 a), such a request should be honoured in a time bound manner.

Data controller is considered to be the first authority and hence he must be approached first rather that approaching the national supervisory authority or a court directly. The formal requirements for a legally relevant request to a controller, especially whether or not it must be a written request, ought to be regulated by national law. Data subject must be responded within the time frame provided by national law. National law should, therefore, prescribe a definite time frame which is not too long and also it provides enough time to the data controller to deal with the request.

Before accepting any such claims the data controller needs to be vigilant to verify the identity of the person who requested such information to ascertain if he/she is the actual data subject and not some third party seeking such confidential information and thus avoid a serious breach of confidentiality. Article 12 (a) points out that access to such information needs to be given to the part requesting at a nominal cost. Some nations mandate that such information should be given for free. The law however has provisions to block any misuse of such a service by individuals.

3.6.2 Claims before the Supervisory Authority

When a person who has requested information on his data does not receive a satisfactory response in a given time frame then he/she can go to the national data protection supervisory authority to seek justice. One will need to advise the authority if the data controller/body was obliged to respond and if an adequate response was given.

The outcome of the proceedings needs to be conveyed to the individual who pursued the case. If one does not get a satisfactory response from the authority itself then they can seek further appeal in the court.[84] This applies to the data subject as well as to controllers, having been a party to proceedings before a supervisory authority.

3.6.3 Claim before the court

As per the Data Protection Directive, if a person has made a request to the data controller. And did not get a suitable response they can go to the national court. [85] However it is recommended that they appeal to the supervisory authority before approaching the court as it will be easier to address their issues. The judgement issued by the supervisory authority can also help to pursue the case in the higher court by the litigant.

Under EU law, individuals whose data has been breached may also approach the CJEU for a suitable judgement in the following cases-

- If the data protection of the plaintiff has been breached by an ancillary body of the CJEU they can appeal to it.
- If the data protection rights of Article 16 of TFEU are infringed by an EU institution while processing data, such a case can also be sent to the General Court of CJEU.

3.6.4 Sanctions

As per Article 24 of the Data Protection Directive the Member States, need to follow all the clauses stated in the Directive and also have remedies for any breaches that might occur. Member states can be free on choosing the remedies that they wish to for noncompliance. As per the CJEU national law is not given full freedom to choose

[84] Data Protection Directive, Art. 28 (4) , available at www.dataprotection.ie.
[85] Data Protection Directive, Art. 22, available at www.dataprotection.ie.

remedies. Disciplinary action is prescribed by CJEU in case where any breach amongst EU bodies is done in accordance with the EU Institutions Data Protection Regulation. This is covered under Article 49, wherein any noncompliance due to any negligence or otherwise, makes the concerned person liable for disciplinary action against them.

3.7 TRANS-BORDER FLOW OF THE DATA

The Data Protection Directive allows for a natural flow of Data between the Member States however there are certain laws that come when it comes to transferring data to non-Member Countries. The CoE has addressed this point in another Additional Protocol to Convention 108 enacted in the year 2001, which became the main regulatory feature on trans-border data flow. Article 25 (1) of the Data Protection Directive deals with regulations for transfer of data to third countries for both pre-processed data and raw data which is to be processed.

In *Bodil Lindqvist*,[86] the CJEU held that "the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes 'the processing of personal data wholly or partly by automatic means', within the meaning of Article 3 (1) of Directive 95/46". There is also provision to allow member states to keep a track of the data which is sent to third countries.

It may be noted that the mere publication of personal data cannot be treated as a trans-border flow and it applies to online public registers or mass media (such as e-newspaper and television) also. Only data which is aimed at specific people who receive the data is eligible under this clause.

[86] CJEU, C-101/01, Bodil Lindqvist, 6 November 2003, available on curia.europa.eu

3.7.1 Free data flows between Member States

Article 1 (2) of the Data Protection Directive is broader in nature and increases the spectrum of trans-border data flow. It also includes EEA countries like Iceland, Liechtenstein and Norway under its ambit and treats these countries as internal market. Article 12(2) allows free flow of personal data between parties to the convention. Domestic law cannot put impose restrictions upon the free flow of data to an external contracting party unless the data is of a very specific sensitive nature. [87] As concerns CoE law, all areas are included within the scope of Convention 108 and the Additional Protocol to Convention 108, although exemptions may be made by the Contracting Parties. All members of the EEA are also Parties to Convention 108.

3.7.2 Free data flows to third countries

Transfer of personal data to non-member countries is said to be free from any prohibition under national law if –

- There are adequate safeguards at the disposal of the receiver for data protection, or
- It is necessary to keep the data subject's interests and interests of other such as important public interests.

1) Adequate Protection

Free flow of data to external countries is considered in Article 25 (1) stated in the Data Protection Directive. Article 25 (6) mandates that European commission needs to have competency to gauge the level of data protection standards in other countries by researching them. The findings stated by the European commission would be deemed as final. The Commission would be publishing its findings in the Official Journal of the European Union and all the member countries of EEA are bound to follow the decision. The commission's published list itself is enough and no further verification is required to be made.

[87] Convention 108, Art. 12 (3) (a).

One of such example can be the Safe Harbour Privacy Principles under which corporates can voluntarily take up membership. These principles were elaborated between the EU and the US for US business companies. Safe Harbour is kind of Code Of Conduct with which if the agencies agree can register and take membership. The Safe Harbour Privacy also comes with an element of state monitoring from the US Federal Trade Commission, and only those companies can join the Safe Harbour, which are subject to the supervision

2) Free Data Flow in Specific Cases

Article 26 (1) has provisions which run parallel to the Additional Protocol to Convention 108.As per this interest of the data subject upon their data flow to third country may be justified if –

- The data subject openly gives consent to data being exported to other countries.
- The data subject is contractually bound to send data to another country
- There is a contract between data controller and an external agency which is sealed in the best interests of the data subject.
- Data transfer is mandatory to safeguard the data subject.
- There is necessary data transfer from public registers and it in the interests of transparency that general public is allowed to access the same. [88]

3.7.3 Restricted data flows to third countries

The Data Protection Directive and the Additional Protocol to Convention 108 permit domestic law to establish regimes for trans-border data flows to third countries not ensuring an adequate level of data protection, so long as the controller has made special arrangements to ensure adequate data protection safeguards at the recipient and so long as the controller can prove this to a competent authority. This requirement is clearly mentioned only in the Additional Protocol to Convention 108;

[88] Data Protection Directive, Art. 26 (1) (d) , available at www.dataprotection.ie.

however, it is also considered to be standard procedure under the Data Protection Directive. The trans-border data flow depends upon the clauses laid in the agreements made between EU Member States and third countries. Examples of such clauses can be as follows:

1) Contractual Clauses

In accordance with the EU standards the European commission with assistance of Article 29 Working Party has formulated set of contract based clauses which are officially certified by Commission Decision as a proof of adequate data protection. [89] The commission's decision is binding to the member states. In case of trans-border data transfer, the data controller and the data receiver in external non-member country need to sign these clauses in order assure authorities that the data protection methods are adequate. The vital components of these clauses are-

- Third party beneficiary clause can allow the data subject to enforce their rights even though they were not a part of the contract.
- The data recipient of third country agrees to comply with the regulatory standards of the exporting country including national supervisory authority and/or courts in case of dispute.

It may be noted that data transfer in between controllers are regulated by two clauses, whereas data transfer between data controllers and processors is regulated by one clause.

2) Special international agreements

The EU has concluded special agreements for two types of data transfers:

- Passenger Name Records

[89] Data Protection Directive, Art. 26 (4), available at www.dataprotection.ie.

Passenger Name Records (PNR) refers to the data obtained by flight carriers as part of reservation. This usually includes data such as name, address, email, bank card details, phone number etc. As per the prevailing law in the US, all airline carriers need to strictly report passenger details to the US homeland Security even before a flight coming to or going from the US. The European Union runs a similar program, called the 'PNR package' which was adopted in 2004.

Post the CJEU's revocation of the 'PNR package', the European Union and the US signed separate agreements to give legal protection of PNR data amongst the authorities that it is shared. Beyond this the mission of the agreements was to ensure that there is adequate infrastructure and policies in place for data protection in countries where the data was getting transferred.

The new agreement signed offered significant improvements. It restricts and clarifies the purposes for which the information may be used, such as serious transnational crimes and terrorism. According to this new agreement data can be stored only for a period of six months beyond which it needs to be deconstructed and left. Data should not be misused for any illegal activities as prescribed under the US law. Individuals have full authority to view their PNR data and in case it is inaccurate they can ask the US department of Homeland Security to rectify it or even erase it. The agreement was ratified in 2012 and will remain in force till 2019.

In December 2011, the Council of the European Union officially authorized, EU Australia Agreement on the processing and transfer of PNR data. The agreement proved to be a benchmark in setting up PNR data best practices guidelines at an international level and also navigating agreements with other countries.

- Financial messaging data

The Society for Worldwide Interbank Financial Telecommunication (SWIFT), based in Belgium, is the establishment behind all global money transfers between banks

worldwide. It was operating with a parallel centre in the US and was confronted with the request to disclose data to the US Department of the Treasury for terrorism investigation purposes.[90] From the EU point of view, there was no sufficient legal basis for disclosing these considerable European data, which were available in the United States only because one of SWIFT's data service-processing centres was located there. Another special agreement was concluded in 2010 between EU and the US referred as the SWIFT agreement, to provide the necessary legal basis and to secure adequate data protection to financial data.[91]

As per this the SWIFT data can be given to US Treasury Department for the purpose of prevention, investigation, detection, or prosecution of terrorism or any terrorist financing etc. The US Treasury Department can seek financial data from SWIFT if it meets below parameters-

- Identifies the particular financial data set that it needs
- Justifies the data needed.
- Request is narrow in nature so that there is a small amount of data that is being asked for and not a big chunk of it.
- It does not ask for any ancillary information such as the Single Euro Payments Area (SEPA)

European government should be furnished with a copy of the original request seeking data so they can judge whether SWIFT principles are complied with. SWIFT after confirming the parameters should provide any authorized data straight to US Treasury Department and not through any intermediary.

[90] Article 29 Working Party (2011), Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing,

[91] European Council's decision of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program.

The financial data needs to be stored in separate and safe data centres wherein the data is secure and also it can be accessed by officials actually investigating the data to reach a conclusion. SWIFT can store financial data it receives not more than five years. Financial data which are relevant for specific investigations or prosecutions may be retained for as long as the data are necessary for these investigations or prosecutions. The US Treasury department can choose to transfer data to any of its agencies inside or outside the country it wishes to, only for the purpose of investigation, detection, prevention or prosecution of terrorism and its financing or public security. Transfer of financial data of EU resident needs consent from competent authorities before the transfer. The SWIFT agreement was valid till 2015with unlimited renewal for a year each time till any party seeks to not renew it by giving six months' notice to the counterpart.

3.8 OTHER DATA PROTECTION LAWS IN EUROPE

Certain legal instruments are adapted and present at the European Convention such as –

3.8.1 Electronic communications

CoE issued a recommendation for data protection specifically for communications field with particular reference to telephone services in 1995. [92] It mandated that personal data being collected should only be for network usage and making telecommunication services available to users eg billing, operations etc. Particular attention was given also to the use of communications networks for sending direct marketing messages. For automated calling devices which are used for mass advertising they should only be used if the consumer has given his/her express consent to it. Domestic law shall provide for detailed rules in this area.

[92] CoE, Committee of Ministers (1995), Recommendation Rec(95)4 to member states on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, 7 February 1995.

The Directive concerning privacy and electronic communication was enacted in 2002, and some changes were made in the year 2009 in order to complement the provisions laid down in Data Protection Directives for telecommunications. The Directive on privacy and electronic communications differentiate three main types of data generated in the course of a communication:

- Strictly confidential data- This data refers to the messages shared in private conversations.
- Traffic data-This data concerns data which is used for maintaining telecommunications operations.
- Location data- This data concerns location of telecommunication devices (particularly relevant to mobile device location) and also other ancillary data concerning users of these devices.

Traffic data is usually used for billing consumers and providing adequate service. However, such data may be disclosed to controllers for offering other premium services such as the next metro station from the user's location or pharmacy or the weather forecast for user's location. These can be important facts related to a person's location and nearby places of business. The amendments to the Directive for electronic communications in 2009[93] were,

- Restrictions on sending SMS, MMS and other similar messages for direct marketing which also covers emails being sent out. These all activities are prohibited unless prior consent is taken from the user.
- Member states need to ensure that there are legal remedies for sending unwanted communication. [94]

[93] Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector
[94] Article 13 of the amended Directive.

- Cookies on online portals should only be allowed to track user information after taking consent from user. Further national law must take care about the type of consent to be taken for adequate protection.

In case there is any data breach due to illegal access or loss of data, the supervisory body must be immediately informed and beyond that subscribers should also be notified where possible damage to them is the consequence. The EU Member States shall designate independent public authorities which are responsible for monitoring the security of the retained data. Surveillance methods of any kind are prohibited and only allowed in case of certain exceptions such as national/state security, protecting rights of data subject, public safety, the monetary interests of the state or the suppression of criminal offences etc.

3.8.2.Employment data

There is no specific statute under EU that deals with employment data. However, when an issue related to employment is concerned, Article 8 (2) of the Data a Protection Directive is usually referred which deals with the processing of sensitive data. One kind of monitoring that exists is the monitoring of communications of an employee at the workplace. The only solution to it is barring private use of communication facilities at work place which seems unrealistic at the same time.

CoE Employment Recommendation states that personal data collected for employment commitments should be obtained from the employee itself. Any data taken at time of recruitment should be only restricted to key information to gauge candidature of the employee. Also judgmental data taken relating to the performance or potential of individual employee should be fair based on honest evaluation.

Sensitive Data taken during employment should be taken only to determine if the person is employable in accordance with the domestic law. Other information such as health related details or medical examination etc. may be asked only if necessary to determine

their eligibility for the employment. Employees should be informed as to how their data will be processed, stored and the entities to whom data are regularly communicated along with the purpose of such communication. In case the company is changing to automated data processing solutions, the employees should be informed even of that. As in other cases, employees should have full access to view and change any of their inaccurate data. If an employee is denied access, rectification or erasure of personal employment data, national law must provide appropriate procedures to contest such denial.

3.8.3.Medical data

Medical data is data which is related to health conditions of an individual and are qualified as sensitive data under Article 8 (1) of the Data Protection Directive and under Article 6 of Convention 108. Article 8 (3) of Data Protection Directive authorizes medical data to be processed for preventative medicine, medical diagnosis and also the proper management of services rendered by a healthcare provider.

The CoE Medical Data Recommendation of 1997 in consonance with the principles of Convention 108 goes deeper into medical data processing. [95] The proposed recommendations are in line with those of the Data Protection Directive as concerns the legitimate purposes of processing medical data and confidentiality maintained at all times. Like other statutes even this allows for data access and rectification of inaccurate data. Medical data should not be disclosed to law authorities until it is certain that safeguards are in place and there is not breach of rights of an individual. Additionally, the Medical Data Recommendation there is special protection granted to provision related to medical data of unborn children, disabled people and on the processing of genetic data.

[95] CoE, Committee of Ministers (1997), Recommendation Rec(97)5 to member states on the protection of medical data, 13 February 1997.

Data may be kept for research purposes till a certain period of time. Pseudonymisation and anonymization may be used as an alternative to ensure that both scientific needs and interests of patient are kept in mind. There are discussions of creating a nationwide electronic database of health files[96] to allow for transmission of information for cross border healthcare initiatives. [97] There are many other legislative and other initiatives pending at the EU level regarding personal data in the health sector.[98]

3.8.4.Data processing for statistical purposes

As per the Data Protection Directive, processing data for statistical research purposes also needs to be protected. Article 13 (2), covers the rules surrounding it. The data accumulated should not be used to make decisions about data subjects. Secondary statistics may be used by acquiring previously collected data and forming theories around it. However, it should also be anonymised or pseudonymised before it is transmitted to any external agency. Article 6 (1) (b) of the Data Protection Directive contains rules regarding safeguards for data to be used for statistical research purpose. Statistics bureaus often use such data to frame public policies. Citizens usually have to share data with national statistics bodies. However, it is important that officials working for such bodies are duty bound to maintain confidentiality regarding the data they possess.

Statistical Data Recommendation which was enacted in 1997 monitors statistics usage in public and private sectors. [99] It is important to note that any data which is collected mainly for statistical use may only be used for it. However, data collected for other reasons may be used for statistical studies in the future. Such data shared to other third-

[96] Article 29 Working Party (2007), Working Document on the processing of personal data relating to health in electronic health records (EHR), WP 131, Brussels, 15 February 2007.
[97] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross border healthcare
[98] EDPS (2013), Opinion of the European Data Protection Supervisor on the Communication from the Commission on 'eHealth Action Plan 2012–2020 – Innovative healthcare for the 21st century', Brussels, 27 March 2013.
[99] Council of Europe, Committee of Ministers (1997), Recommendation Rec(97)18 to member states on the protection of personal data collected and processed for statistical purposes, 30 September 1997.

party statistics agencies for any further study is permissible under this Recommendation. However, such parties should agree and write down the extent of the legitimate further use for statistics. It is important to anonymise statistical data for use before it can get transferred for further use.

If a statistical survey using personal data is not prescribed by law, the data subjects would have to consent for the use of their data so as to make it lawful, or they should at least be given a chance to object. If personal data is taken by interviewing people, then they need to be informed beforehand about data collection of data and its distribution. Sensitive data should never be collected in such a way that an individual can be identified unless clearly permitted by national law. After relevant statistical studies are done on the personal data they can be either removed or anonymised. While the encryption keys with other identifying specific data should be stored separately from the anonymised or pseudonymised data.

3.8.5.Financial data

The Convention 108, called for providing clauses surrounding data protection with reference to payments data perspective and such legal framework was developed by CoE in Recommendation Rec(90)19 of 1990.[100] This recommendation makes clear that the scope of legitimate collection and use of data in the context of payments, especially by means of payment cards. The Recommendations guided that the National laws need to ensure data from payment cards is encrypted and that there are fixed procedures surrounding its transparency. It further recommends to the domestic legislators detailed regulations on the limits of communicating payment data to third parties, on time limits for the conservation of data, on transparency, data security and trans-border data flows and, finally, on supervision and remedies. There are various legal statutes that are being

[100] CoE, Committee of Ministers (1990), Recommendation No. R(90)19 on the protection of personal data used for payment and other related operations, 13 September 1990.

formulated to regulate the financial services sector and the activities of credit institutions and investment firms.[101] There are many vital issues surrounding it such as-

- Breach reporting mechanism
- Holding of records of financial dealings.
- Understanding between Member countries and European Securities and Markets Authority (ESMA);
- Surveillance by tapping phone conversations, including the power of the capable authorities to request telephone and data traffic records
- Transfer of personal data to other countries.
- The power of capable authority to seize documents and conduct raids
- the disclosure of personal information, including the publication of sanctions;

There are also other issues in these areas that are specifically addressed, including collecting data on the financial status of data subjects or cross-border payment via banking transfers, which inevitably leads to personal data flows.[102]

[101] European Commission (2011), Proposal for a Directive of the European Parliament and of the Council on the access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms and amending Directive 2002/87/EC of the European Parliament and of the Council on the supplementary supervision of credit institutions, insurance undertakings and investment firms in a financial conglomerate, COM(2011) 453 final, Brussels, 20 July 2011.

[102] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ 2007 L 319.

Chapter : 4

REGULATORY FRAMEWORK OF DATA PROTECTION IN INDIA

Table Of Contents

1. BACKGROUND

India's compliance requirements as far as data protection is concerned, are quite different from other western countries due to its social and cultural settings. The terminologies regarding privacy are based on western thinking and do not take into consideration other socio-historical contexts. There is a wide divide in the cultural context of data protection amongst different nations which is the theoretical evidence behind the ongoing controversy regarding privacy rights. Social ideologies are different and this leads to core foundations of general rules for data protection. Data protection as a whole is more concerned with things such as personal liberty, justice, human dignity, individuality and family life. Data protection is widely acknowledged; however the process of coding data is relatively new. Since societies are dynamically evolving, the need for redefining data protection is much needed.

The differences pertaining to the notion of data protection are the reflection of differences in cultural values and, the role of data protection (specifically privacy rights) as embedded in the India's constitutional tradition. Some people believe that data protection is weak in India as there is no elaborate legislature for data protection but this is not the case. In India, privacy is seen as a matter related only to personal space and individuals.[1] Privacy is a wide term and can have various interpretations depending on socio-economic and cultural conditions. Indian culture is quite distinct from western culture. Culturally, India has never taken communication or information as "private". There is also narrow interpretation of private lives in India, as major part of an individual's life is exposed to and knotted with dependent of a family, a community, a village or a society. The holistic culture of India, which seems to embrace a socio-centric conception of the relationship of the individual with society, is contrary to the western culture.[2] As per Hofstede's model, India is a country where there is a higher power distance index and low individualism index compared to other nations such as U. S and U.K. It is observed that in countries with a collectivist society people in general ten to trust other people than those in individualist societies. [3] Talking about European Countries, an individual is considered as a true entity and an individual block of society.

[1] Ponnurangam Kumaraguru Et Al., Privacy Perceptions in India and the United States: An Interview Study (2005), *available at* www.cs.cmu.edu, visited on 3rd December 2017.
[2] Richard A. Shweder & Edmund J. Bourne, *Does the Concept of the Person Vary Cross-Culturally? Abstract available at link.springer.com*, visited on 10th September 2013.
[3] Hofstede's Book on Cultural Dimensions

Differing to it is Indian culture where an individual is a part of whole and in this wholesome context his existence is defined.[4] Western societies therefore are more aware of data protection rights and concerned that they are well implemented. It is common practice in India for panchayats to discuss a family's personal matter at a public space, with members of the community sharing the views on the matter. In India both individual rights aspect of privacy and social value of privacy, are safeguarded.

In western countries general practitioners (GPs), do not freely discuss medical information of a wife to her husband and vice versa. In India it is a bit different, and medical information is actively discussed amongst all members. In India, privacy is generally seen to be associated with confidentiality and personal space along with sharing of professional, familial or personal information with each other. There is not much emphasis on the economic ramification of loss of privacy. In India since privacy is seen in terms of personal space, people in general do not directly associate it with other forms of privacy such as financial information or identity theft unlike the people of USA.[5] In India, majority of people tend to agree that data privacy is not too important as they believe that they are very transparent and have nothing to hide. The case is opposite in the west, where most of the people agree that data protection is an important matter of concern. When asked about general laws in a survey, Indians did not mention any thing about data protection whereas in America around 14 % people mentioned it.[6] The average of people concerned by threats to privacy due to cell phones equipped with cameras is the same in both countries. This can be explained by the recent incidents related to these technologies both in India and the USA and the media coverage which ensued.[7] These surveys were commissioned by the School of Computer Science at Carnegie Mellon University[8] and revealed that there are different perspectives around the concept of data privacy in all countries. Privacy is not of paramount importance in Indian society compared to Western society.

[4] 'Is the Notion Of Human Rights a Western Concept?' by R. Panikkar
[5] P. KUMARAGURU and L. CRANOR, Privacy Perceptions in India and the United States : An Interview Study, available on www.cs.cmu.edu, visited on 10th September 2013.
[6] "The typical responses of the subjects in India were "No absolutely not. I have never felt a threat to [my] identity" and "No, nothing, I don't have concerns about my identity being stolen". P. KUMARAGURU and L. CRANOR, Privacy Perceptions in India and the United States : An Interview Study, p. 9, available on www.cs.cmu.edu, visited on 10th September 2013.
[7] P. KUMARAGURU and L. CRANOR, Privacy Perceptions in India and the United States : An Interview Study, available on www.cs.cmu.edu, visited on 10th September 2013.
[8] Ponnurangam Kumaraguru & Lorrie F. Cranor, *Privacy In India: Attitudes And Awareness*, *In* PROCEEDINGS OF THE 2005 WORKSHOP ON PRIVACY ENHANCING TECHNOLOGIES (PET 2005: 30 MAY - 1 JUNE 2005, DUBROVNIK, CROATIA), *Available At* Lorrie.Cranor.Org/Pubs/PET_2005.Html;

Before the Constitution of India was enacted, rights of citizens in India were not guaranteed. Before the Constitution, individuality of Indians was determined by common laws. Moreover, the citizen of India got their legal identity of being an Indian citizen only after the enforcement of the Constitution. Criminal Laws gave protection to the person, property and dwelling house and made it punishable to impute un-chastity to a female .There was another law knows as the law of Libel and Slander gave protection to the public reputation of people. While, the law of Torts, gave protection of individual interests in reputation as also the person and property with an admonition that the least touching of another in anger was assault actionable in damages.

The age of Internet has taken on India to new heights of excellence in education, medicine, communication, public services and almost all walks of governance. IT has become a pivotal point in helping India emerge as a world leader in business process outsourcing in various fields, such as telecom, banking, communication etc. India played a key role in the management of the millennium bug where a large part of the work was outsourced in India. As globalization occurred, US companies started outsourcing work to India which came as a boon to the large number of English speaking citizens who earlier had low employment opportunities due to the slow rate of growth. Cheap labour, enter prising and hardworking nature of the people etc. are the other reasons attributed for the development of Outsourcing Industries in India. Outsourcing has become one of the biggest industries in India.

2. CONSTITUTIONAL ASPECT OF DATA PROTECTION

India comprises of twenty-eight States, six Union Territories and National Capital Territory of Delhi. The Constitution grants certain statutory powers to all States. [9] In the 1990s with decentralization of power, each state was given certain powers in accordance with their population size and other factors. The major powers were still controlled by the Central Government. All executive powers are handled by the President and Council of Ministers who help the President on important matters. [10] The role of the President is not too wide. The real powers are under the Prime Minister's disposal. Council of

[9] G. GOVINDA and N. SINGH, "The Political Economy of India's Federal System and its Reform", April 2004, p. 2, available on repositories.cdlib.org, visited on 17th February 2013
[10] Article 73 of the Constitution of India.

Ministers act on behalf of the President, under the guidance of the Prime Minister. [11] They are ultimately accountable to the Lok Sabha.

The parliament of India is made up by two houses- Lok Sabha (House Of People[12]) and Rajya Sabha (Council of States[13]). Legislative power in India is bifurcated into three parts- The Union list which comprises of matters for which only the Parliament can decide upon, the State list contains matters that can only be taken up at State Level and then the Concurrent list which contain issues on which Union and State can decide upon.

The Constitution of the Republic of India was passed on November 26th, 1949. This written Constitution aims to establish - at both Union and State levels - the main organs of the Executive, Legislative and Judiciary powers. It defines the powers of each and acknowledges a separation of powers. Article 246 (1) of the Constitution of India grants the Parliament with the exclusive power to make laws with respect to any of the matters enumerated in List I of the Seventh Schedule.

The Constitution of India embodied Fundamental Rights in Part III, which are enumerated in Article 14-30. Indeed, the Supreme Court deduced that right from the Right to Life and Personal Liberty enshrined in Article 21 of the Constitution through an extensive interpretation of the phrase Personal Liberty. Article 21 states "no person shall be deprived of his life or personal liberty except according to procedures established by law". According to the Supreme Court the idea of personal liberty was living a life which was devoid of encroachments of any kind. Thus, any law like this basically needed to pass a triple test-

- It should be an established procedure in practice.
- The procedure should be compliant of one or more fundamental rights of Article 19 applicable in a situation.
- It should be tested in reference to Article 21 and any such act should be fair and not create any oppression on the victim.[14]

[11] Article 77 of the Constitution of India.
[12] Its composition is the following one : A maximum of 530 Members are directly elected and 20 other Members (this is a maximum) represent the Union Territories."
[13] Its composition is the following one : 12 Members are nominated by the President and the other Members (238 maximum) are the representatives of the States and Union Territories.
14 Maneka Gandhi V. Union Of India

Since 1960, the Indian judiciary is dealing with the issue of privacy either under the shield of fundamental right laid down in Constitution or as a common law right. Courts have not given too much importance to the right to privacy but the Courts have preferred to determine the importance of privacy on a case by case basis.

In the Kharak Singh V/s State of UP, [15] the Supreme Court was to make a decision on whether the police was right in undertaking surveillance of people with a criminal records and making visits. In this case the concerned individual was being troubled by the police who made visits at night under the Regulation 236(b) of UP Police Regulation. The individual challenged it in court stating that they were a violation to his own liberty. The judges objected stating that Article 21 was not part of the fundamental rights granted to the citizens. Only two judges out of seven agreed that irrespective of the position of right to privacy in the Constitution, it still was a basic right which granted liberty. [16] Justice Subba Rao held "It is true our Constitution does not expressly declare a right to privacy as a fundamental right, but the said right is an essential ingredient of personal liberty."

Again, in Govind v. State of Madhya Pradesh, the petitioner, challenged police actions for violating his right to privacy. Again, only partial members of the bench were inclined to interpret it in view of a right to privacy. One of the judges argued that a person's life was free from official intervention in all things except when it was not reasonable to do so. Similar issues were raised in the Kharak Singh case; the three judges hearing this particular case were inclined to grant the right to privacy the status of a fundamental right. Justice Mathew stated: "Rights and freedoms of citizens are set forth in the Constitution in order to guarantee that the individual, his personality and those things stamped with his personality shall be free from official interference except where a reasonable basis for intrusion exists.[17]

In the case of R. Rajagopal v. State of Tamil Nadu, the right to privacy and right to freedom of speech were contradicting with each other. In this case the petitioner was a magazine based in Tamil Nadu which sought aid from court to restraint government officials interfering in the publication of the autobiography of a death row convict–

[15] AIR 1963 SC 1295
16 Kharaksingh V. State Of Uttar Pradesh ((1964) SCR (1) 332)
17. Govind V. State Of Madhya Pradesh (AIR 1975 SC 1378)

'Auto Shankar' which contained details about the nexus between criminals and police officers. The Supreme Court had to deal with issues such as if freedom of speech gave authorization to publish an account of a citizen's life without any consent. The Supreme Court had to deal with the questions like: "Whether a citizen can prevent other citizen from publishing his or biography? Does the freedom of speech and expression guaranteed by Article 19(1) (a) entitle the press to publish such unauthorised account of a citizen's life and activities and if so to what extent and in what circumstances?" The Supreme Court was of the opinion that Right To Privacy should remain at individual level and should not be mixed with matters of a public domain. The Supreme Court held:

- "The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a "right to be let alone". A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child-bearing and education among other matters. None can publish anything concerning the above matters without his consent. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages.
- The rule aforesaid is subject to the exception, that any publication concerning the aforesaid aspects becomes unobjectionable if such publication is based upon public records including court records. This is for the reason that once a matter becomes a matter of public record, the right to privacy no longer subsists and it becomes a legitimate subject for comment by press and media among others."[18]

In the case of (People's Union for Civil Liberties) PUCL v. Union of India, [19] the issue of unauthorized tapping into phone calls was asked. The court was of the opinion that tapping telephone calls was a breach of privacy. Moreover, it is expected that the intelligence cell of the government will try to gather information using such means; however citizen's right to privacy has to be protected from being abused by the authorities of the day. It would be a clear violation of Article 21 of the Indian Constitution.[20] In the case of Pooran Mal v. Director of Inspection (Investigation) of Income-tax, New Delhi, [21] the court categorically states that searches done by the

18 R. Rajagopal V. State Of Tamil Nadu (1994 SCC (6) 632)
[19] (1997) 1 SCC 30
20 PUCL v.s Union of India ((1997) 1 SCC 30)
[21] AIR 1974 SC 348

government body to gather evidence would not be a violation as there is no fundamental right to privacy. (This would tend to weaken the right to privacy by allowing a public authority to use evidence obtained illegally.)

The blood donor's right to privacy of his medical records was discussed by the Supreme Court in the case of **Mr. 'X' v. Hospital 'Z'.**[22] Doctor-patient relationship is a matter of confidence and therefore, doctors are morally and ethically bound to maintain confidentiality. In certain circumstances, Right of Privacy may lead to the clash of one person's "right to be let alone" with another person's right to be informed. Situations where public interest would override the duty of confidentiality, for example, one person's disease may cause health risks to others in such situation confidentiality should not be given importance. Here in this case, the respondent hospital had disclosed without the permission of the blood donor, the fact that the blood donor was diagnosed as HIV patient. Such disclosure broke off the engagement of the blood donor with his fiancée and the donor was subject to social ostracism. Discussing the issue of privacy of medical records, the Supreme Court ruled that while medical records are considered to be private, doctors and hospitals could make exceptions in certain cases where the non-disclosure of medical information could endanger the lives of other citizens, in this case the wife.

In the case of **District Registrar v. Canara Bank**[23] the Supreme Court came up with the milestone judgement imparting importance to privacy. The Supreme Court was required to determine the constitutionality of a provision of the A.P. Stamps Act which allowed the Collector or 'any person' authorised by the Collector to enter any premises to conduct an inspection of any records, registers, books, documents in the custody of any public officer, if such inspection would result in discovery of fraud or omission of any duty payable to the Government. The impugned provision was held to be unconstitutional by the Supreme Court on the grounds that it failed the tests of reasonableness enshrined in Articles 14, 19 and 21 of the Constitution.

The court held in the Maneka Gandhi v. Union of India case that law obstructing the right to privacy should satisfy triple layer test-

- It should be an established procedure in practice.

[22] AIR 1999 SC 495
[23] (2005) 1 SCC 496

- The procedure must be compliant to test one or more clause of Article 19.
- It should also be compliant while testing clauses of Article 14.

The Court stated that such a right mainly concerned the people irrespective of the place. Therefore, whether the financial data was kept in home or at the bank, the mere fact that the data was of private individuals guarantees protection under national law at all times.[24]

In the case of Peoples Union for Civil Liberties (PUCL) v. Union of India, the right to privacy was not violated when criminal records regarding an electoral candidate were published. It was determined that the rights of people to know the candidate's history were more vital than the right to privacy of the electoral candidate. [25]

In the case of the Naz Foundation, the Delhi High Court held that the right to privacy has been held to protect a 'private space in which man may stay what he is. He remains himself the way he wants to be'.[26] The judges took right to privacy as a concept of dignity and its existence in Indian Constitution. The court observed that dignity requires valuing the worthiness of an individual as a part of our society. Naz Foundation enunciates an exceptional non-spatial and convenient understanding of privacy that extends beyond "place" into "person". It is clear that the Indian culture of privacy is dominated by such factors as rights of the family, observation of the "purdah" and the belief that intrusion affects the modesty, dignity or decency of the person

Hence under the light of above discussed case laws it is quite evident that, privacy was never "less valued" in Indian culture; it is seen more as part of a "societal value" rather than an "individual value". It confirms that Indians are more concerned with a not the same dimension of privacy and attribute value to protecting the concerns that fall within that dimension. Privacy under Indian culture is not seen as an "essential element" but as "contributory element". India is not a society deprived of importance of privacy – but it has a diverse acuity of privacy from that to which we have become accustomed in the West. India's attitude toward privacy is more of "respect", rather than a right. Privacy in India is more about practical rules based on "social ethics", "virtues" and

24. District Registrar v. Canara Bank ((2005) 1 SCC 496)

25 Peoples Union for Civil Liberties (PUCL) v. Union of India, AIR 2003 SC 2363

[26] Naz Foundation v Government of NCT of Delhi WP(C) No.7455/2001 (2 July 2009).

"righteous" conduct. This attitude is compatible with the social and cultural structure of the country where a high level of privacy is seen to have a detrimental effect on the trusting relationships and social interaction with others.

3. REGULATARY ARENA FOR DATA PROTECTION UNDER INDIAN LAW

Data protection law in India comprises of civil and criminal liabilities. Data theft is considered a violation of privacy and therefore attracts both civil as well as criminal liabilities. Since 2000, attempt has been made to cover the right to privacy under IT Act, 2000. This was the first time data stored was also included under the ambit of data protection. The legislature included the Personal Data Protection Bill in the year 2006, to provide adequate safeguards. Beyond this a Right to Privacy bill was also introduced by the Parliament soon after

3.1 PROVISIONS AS PER INFORMATION TECHNOLOGY ACT

The Information Technology Amendment Act, 2008, made up for lost ground in data protection laws in India. However, these laws were bit inadequate and did not address the issues for the corporate sector. Companies in India, especially the ones into outsourcing, have lots of critical data at their disposal which includes lot of personal data such as bank card details, health records etc. All this data at the hand of employees makes it a bit risky. The data can be used to intimidate people. Historically there have been cases where employees stole data thus breaching security and causing mistrust amongst Indian companies for handling data.

As per the Information Technology Act, data means any unprocessed information. Information means data that is organized in a systematic manner and communicated for easier understanding. All information is stored in network of computer. This information means financial details, health information, business proposals, intellectual property, etc. Until now there was no specific provision for this. However, after the Information Technology Amendment Act 2008 it came into being.

3.1.1 INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act governs data protection in India. It was enacted on 17th Oct, 2000. This Act's foundation was the Resolution A/RES/51/162 adopted by the General Assembly of the United Nations which was based on model law; in force via United Nations Commission on International Trade Law (UNCITRAL).There were three primary aims behind the Information Technology Act-

- To enable a safe environment for development of ecommerce by giving appropriate tools and infrastructure for transactions.
- To adopt the use of digital signatures for verifying documents stored in electronic records.
- To promote the IT sector and the government's role in supporting it.

The Act primarily covers "e-commerce" and "e-governance" and many parts ancillary to it eg hacking, digital signatures information in electronic form, computer crime, damage to computer source, breach of confidentiality and viewing of pornography. Data protection is mainly covered by the Information Technology Act, 2000.

The IT Act defines the term 'data' as, "data means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer". The provisions dealing with this data are primarily-

Section 43. Penalty for damage to computer, computer system, etc.

The section mainly covers unauthorized use of computer systems. So, if a person without consent of the owner / person in charge of system / network -

- Accesses any such system or network.
- Downloads data, copies it or extracts information from computer, its system or network via other forms of storage (such as removable storage medium).
- Tries corrupting the computer with virus into computer, its system or network.

- Causes any damage to computer, network etc.

It covers civil liability for any kind of data theft on computers, illegal downloading, computer database, theft of data, unauthorized transmission etc. To be precise this section provides protection against unauthorized access of the computer system by imposing heavy penalty which can be up to one crore. Clause 'c' covers matters related to corrupting the computer network etc. Clause 'g' covers penalties for anyone giving illegal access to the unauthorized.

Section 65. Tampering with computer source documents

If anyone indulges intentionally in trying to hide, alter or destroy computer source code when the computer source is to be kept or maintained by law, then such people are punishable whether they did such an act knowingly or unknowingly with imprisonment upto three years, or fine which may extend upto rupees two lakhs or both. Computer Source Code under this section can be taken as the listing of programs, computer commands, design and layout and program analysis of computer resource in any form.

Section 66. Hacking with Computer System

This clause states covers-

- People, who have the intent to cause any loss, alter or damage to public by changing any information in the computer source to reduce its value, is said to have committed hacking.
- Anyone who is caught trying to hack into systems might face three years of jail and a financial penalty which can be extended to rupees three lakh.

Hacking is being taken care under this section. Hacking is considered the act of intentionally causing loss to any person or any information in the computer which will ultimately destroy its overall value. Eg if any data contains a secret personal id and if that is extracted, then the whole document becomes pointless. This section imposes the penalty of imprisonment of three years or fine up to two lakh rupees or both on the hacker. Here the term diminishes / reduces its value or utility points towards the importance of the confidentiality of a document.

Section 70 Protected System

Protection of data stored in protected system is covered under this section. Protected systems are those computers, computer system or computer network to which the appropriate government, by issuing gazette information in the official gazette, declared it as a protected system. Anyone trying to access it illegally will face imprisonment which may extend upto ten years and also a fine.

Section 72. Penalty for breach of confidentiality and privacy

This section states that any person who has secured an illegal access to electronic records, documents etc. without the consent of its original owner may be liable for jail which can be extended upto two years and a fine which can be extended to one lakh rupees or both. It may be noted that this is the singular section that deals with consent of individuals. Indeed, this section confines itself to the acts and omissions of those persons, who have been conferred powers under the Act, rules or regulations made thereunder.

These authorities are:

- The Controller responsible for Certifying Authorities,
- The Deputy and Assistant Controllers managing Certifying Authorities,
- Authorized (Licenced) Certifying Authorities,
- The Adjudicating officer,
- The Presiding Officer of the Cyber Appellate Tribunal,
- Registrar of the Cyber Appellate Tribunal,
- Network Service Provider, and
- Police officers (DSP)

Most of these roles have conferred powers so in practical aspect the number of data controllers is limited. The dual advantage of this section is that it gives respite against any potential breach of confidentiality and also puts focus on data privacy. It may be noted that any person who has the power to access electronic records, registers, information etc. and discloses critical details to another person may be imprisoned which can be extended upto two years and face a fine extended up to a lakh of rupees or both.

The Information Technology Act, 2000 was not perfect and had its own flaws. The

Information Technology Act, 2000 is a bit generic and deals with issues of data protection in a very superficial manner. Beyond this the Act does not explicitly define as to what constitutes personal data. Data as per se under the IT Act is more relevant in cybercrime compared to normal privacy matters. The Act did not give comprehensive data protection or transparency in data. Hence the Government of India had in the year 2006 introduced a separate Bill called the Personal Data Protection Bill to specifically address the issue of data protection.

3.1.2 PERSONAL DATA PROTECTION BILL 2006

The personal data protection bill 2006 was a simplistic 14 section bill according to which personal data should not be collected without authorization and should never be disclosed for any marketing and /or commercial gains. Central and State Government could refine the law further for the data controllers in their territory. Each state could assign up to three data controllers for their territory. Appropriate exemptions were doled out maintaining security and minimum data collection standards. Reporting to the Data Controller and mandating security and minimum collection principles were also indicated. As far as disciplinary action is concerned, imprisonment of three years and up to Rs 10 lakh was deemed to be payable to any such victim. The Act did not get launched but it did result in rectification of Information Technology Act, 2008. Vicarious liability of corporate personnel was also included. Summary trial under CrPC was recommended for grievance Redressal. However, the Bill has not seen the light of the day. But it resulted into the amendment to the Information Technology Act and now the issue of data protection has been addressed in Information Technology Amendment Act, 2008.

***3.1.3** THE INFORMATION TECHNOLOGY ACT, 2008*

The Department of Information Technology, the Ministry of Communications and Information Technology and the Government of India established an Expert Committee on Information Technology, 2000.[27] The recommendations of the same were handed over to Government of India and are currently held by the Ministry of Law and Justice for further review. One of its terms of reference was "to consider and recommend suitable legislation for data protection (privacy) in the Information Technology Act, 2000".

27 notification no. 9(16)/2004 –EC dated January 7, 2005

The committee gave its report in August 2005 to the Department of Information Technology. According to the committee, sections 43, 65, 66 and 72 need to be reviewed in terms of data protection and privacy. It gave the following recommendations. Besides any contractual agreements in amongst parties the Sections (viz. 43, 66 and 72) have been revised. The main pointers being-

- A new Section 43(2) revolves around handling sensitive personal data and appropriate security practices.
- Grading of computer related offences in accordance with their severity under Section 66.
- Further refinement of Section 72(1)
- New Section 72 (2) to be adopted in light of any breach of confidentiality which could cause damage to the victim.

Language of Section 66 about computer related offences has further been revised to align it with Section 43. These have been graded with the degree of severity of offence when done by any person, dishonestly or fraudulently without the permission of the owner. It may be noted that following sections are put into IT Amendment Act, 2008:

- Section 43A –Compensation when there is a failure to protect data
- Section 66 –Computer related offences.
- Section 66A – Disciplinary action for sending anything offensive through communication networks.
- Section 66B –Punishment for being in possession of any stolen computer device.
- Section 66C –Punishment for any identity theft which occurs.
- Section 66D –Punishment for cheating by personation by using computer resource
- Section 66E – Punishment for any violations related to privacy.
- Section 66F – Punishments for anyone involved in cyber terrorism
- Section 67 –Action against those found sending obscene materials via electronic forms.
- Section 67A – Punishment for publishing any materials containing sexually explicit act, etc. in electronic form
- Section 67B – Punishment for publishing or transmitting of material showing children in sexually explicit act, etc. in electronic form
- Section 67C – Preservation and Retention of information in possession of

intermediaries.

- Section 69 – Powers to order for interception or monitoring or decryption of any information through any computer resource
- Section 69A – Power to order blocking for public access of any information through any computer resource
- Section 69B – Power to sanctioning, monitoring and collection of traffic data or information through any computer resource for cyber security
- Section 72A – Punishment for Disclosure of information in breach of any lawful contract done
- Section 79 – Exemption from liability of intermediary in certain cases
- Section 84A –Modes for encryption
- Section 84B –Punishment for abetment of offences
- Section 84C –Punishment for attempting to commit any offences[28]

Section 43 A reads as follows: (Compensation for failure to protect data)

According to this any body/corporate in possession of sensitive data, which does not maintain adequate safeguards for data protection and by doing so causes harm to people, shall be liable to give compensation for the same. Out here personal data is defined as any information with details of a personal nature. The definition may be decided by the Central Government in consultation with other professional bodies or associations it may deem fit. Here body corporate refers to any firm or sole proprietorship which is conducting commercial or professional activities. Reasonable security practice and procedures concerns information which is needed to adequately protect data from illegal access, damage, unauthorized changes etc.

This section primarily contains details of provisions laid down by way of agreement between two parties for the inflow of data. The contracting parties need to explicitly define as to what kind of security are they demanding. For any breach of contract damages not exceeding rupees one crore need to be paid to the affected victim. The amendment brought to the Act has not precisely defined the meaning of "sensitive personal data" and just states that it would mean personal information however, the term may be defined by the Union Government after consultation with relevant bodies.

28 Article By Vijay Pal Dalmia, Advocate

Section 66 Computer Related Offences (Substituted vide ITAA 2008)

This section was replaced by the through Information Technology Amendment Act, 2008. The section reprimands people for any act done with fraudulent intentions. The punishment could be jail up to 3 years maximum or fine which may be extended to rupees 5 lakhs or both. Section 66 A deals with offensive messages sent via communication mediums. Section 66 A sub-clause (c) was included vide Information Technology Act, 2008 and concerns electronic mail message which causes annoyance or alternatively is misleading the person about its true origins.

Section 66 B Punishment for dishonestly receiving stolen computer resource or communication device (Inserted Vide ITA 2008)

This section concerns punishment for a person who receives or retains any previously stolen computer resource or communication device. Punishment for such an act could be up to 3 years maximum imprisonment or one lakh rupees maximum fine or both.

Section 66 C Punishment for identity theft. (Inserted Vide ITA 2008)

This section primarily concerns punishment for any person for committing fraud by using the password, electronic signature or any other unique identification feature of any another person. The punishment for this offence could be imprisonment which can be extended up to 3 years and a fine which may be up to rupees one lakh. The term dishonesty refers to anything done for wrongful gains to one and harm to another one, whereas the term 'frequently' represents when a person does a thing with an inherent intention to defraud.

Section 66 D Punishment for cheating by personation by using computer resource (Inserted Vide ITA 2008)

This section deals with people who cheat others using communication devices or other computer resources, who shall be punished with imprisonment which may be extended till three years and they shall be liable to fine which may extend up to rupees one lakh.

Section 66 E. Punishment for violation of privacy. (Inserted Vide ITA 2008)

This section primarily deals with people who are involved in capturing and transmitting images of private part of a person without any consent from the person thus violating his/her personal privacy and such person shall be punished with imprisonment which

may extend to three years or with fine not exceeding two lakh rupees, or with both. Here, 'transmit' stands for sending visual images electronically and capturing stands for recording of material for example videotape, photograph, film, etc. The term "Private Area" includes any such image which is immoral or against the law prevailing in India.

Section 66 F. Punishment for cyber terrorism

According to this section any individual who tries to cause a threat to the unity, integrity, security or sovereignty of India, through unauthorised access to computer resource or causes any computer contaminant which results to causes or likely to cause death or injuries to persons at large or may cause damage to property is liable under the charges of cyber terrorism. Cyber terrorism also includes any illegal access computer resource through which one can obtain information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise. Any person who gets charged under cyber terrorism may get imprisonment term for life.

Section 66 is regarded as the foundation of criminal sentences for matters related to cyber terrorism. This section has been inspired by Section 43 of the Information Technology Act; 2000.Section 66 also aligns itself to laws under the European Convention on Cyber-crime. The word dishonestly under this section means whenever an action is done to get wrongful gain while the word fraudulent implies something done with intention to defraud. And the term "Without the permission of the owner" shall include access to information that exceeds the level of authorized permission to access.

Section 67 Punishment for publishing or transmitting obscene material in electronic form (Amended vide ITAA 2008)

As per this section anyone who transmits any obscene or forces anyone else to transmit such in an electronic form shall get an imprisonment till 5 years and fine of Rs 10 lakhs

or both. It may be noted that this section does not apply to other forms such as publication, marketing pamphlets, literature etc as there might be some proper justification for the same.

Section 67 A Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form (Inserted vide ITAA 2008)

This section punishes those who publishes or transmits or make other to publish or transmit in an the electronic form any material which contains sexually explicit act or conduct for first conviction with imprisonment which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment which may extend to seven years and also with fine which may extend to ten lakh rupees. However, protection of section 67 is not extended to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic from on the basis that such publication is justified as being good for the public with reference to the interest of science, art, literature, art, or learning or other objects of general concerns.

Section 67 B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.

As per this section anyone who transmits or makes someone else publish any obscene material featuring kids engaged in such activities through any form, technology, digital etc, promotes much material will be liable for punishment with imprisonment which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment which may extend to seven years and also with fine which may extend to ten lakh rupees. The punishment is for both one who publishes or transmits as well as the one who is made to publish or transmit. Anyone who forces kids to have relationship and makes them involved in such acts is also liable under this section. Punishment will be imprisonment which can be extended up to 5 years and fine up to Rs 10 lakhs maximum. If there is any subsequent conviction the imprisonment term would be seven years and fine up to Rs 10 lakhs.

Section 67 C Preservation and Retention of information by intermediaries

As per this section, any Intermediary should preserve information as per the terms stated by Central Government. Any intermediary, who goes against the norm, will be

punished with an imprisonment term up to three years and also liable to fine.

Section 69 Powers to issue directions for interception or monitoring or decryption of any information through any computer resource (Substituted Vide ITAA 2008)

As per this section any officer authorized by government who feels that for the purpose of investigation it is required to intercept, monitor or decrypt communication through computers in the best interest of the country's sovereignty, relationship with foreign countries etc then, such an act may only be deployed by any individual assigned by the government or agency doing it on government's instructions Such agency will have access to all types of information whether secure or insecure.

Section 69 A Power to issue directions for blocking for public access of any information through any computer resource

As per this section any individual assigned by government may block access to any information to the public that is transmitted, stored, received etc if it feels that is it is critical to ensure that information should be blocked in the interests of the country, its relationship with other nations etc. Such an act may only be deployed by any individual assigned by the government or agency doing it on government's instructions Such agency will have access to all types of information whether secure or insecure.

Section 69 B Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security

As per this section the central government to improve Cyber security and analyse data intrusions etc may authorize agencies to collect and monitor web traffic data by stating the agency name in the official gazette, Here "traffic data" refers to any particular data identifying an individual or computer resource through which other details may be obtained, eg date, size, time route, point of origin etc,

Section 72A: Punishment for Disclosure of Information in Breach of Lawful Contract.

Section 72A, is a relatively new provision, and deals with any data leaked resulting from the breach of contractual agreement. It states that any intermediary who has possession of data identifying people while providing services, and who has an evil

intention to cause damage to the contracting party by disclosing data, may be liable for imprisonment which can be extended upto 3 years with a fine extended upto five lakh rupees or both,

Section 75 Act to Apply For Offences or Contraventions Committed Outside India

This section deals with the issues such as the applicability of the act outside India's geographical area. According to this section, the IT Act will apply to any person regardless of nationality if the offence involves a computer system or network in India. This clause has been formulated to assist in fighting cybercrime. As per this organizations which store personal data need to necessarily register with the Information commissioner appointed as a government official. There are some restrictions on collection of data. The data must be obtained always legally and shall not be obtained for any manner incompatible with other purposes. Personal data should be sufficient for the purpose it was collected for.

Section 79 Exemption from liability of intermediary in certain cases (corrected vide ITAA 2008)

As per this section, the intermediary needs to carry out the plan of action according to the norms set by the government. It must follow instructions of the government. The intermediary will not be liable for any third-party information, data or any external link which is hosted by them. The provisions do not apply if intermediary is involved in any criminal conspiracy. When any communication link provided by the intermediary is being used for unlawful activity, the intermediary is ultimately responsible. If such an illegal instruction is spotted the intermediary must take all steps to disable access to such data. The provisions of this section applies only if the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored.

Section 84 Protection of Action taken in Good Faith

No legal case should be put against the Central government, State government, the Controller ot any other person acting on behalf of him for an act done in good faith and in pursuance of this Act or any rule, regulation or order made there under..

Section 84 A Modes or methods for encryption (Inserted Vide ITAA-2008)
Central government may secure the platforms for e-commerce, e-governance etc and accordingly specify the methods of encryption.

Section 84 B Punishment for abetment of offences (Inserted Vide ITAA-2008)
Whenever an individual helps another one in a criminal act and there is no specific provision made by the act, the person will be punished with the punishment in accordance with the offence. It covers even any act which is committed as part of assisting criminals.

Section 84 C Punishment for attempt to commit offences (Inserted Vide ITAA-2008)
Whenever any person commits an offence, or which is punishable by the act or causes another person to commit criminal act and no explicit provision is made for the act, the person may get a jail term up to one half of the imprisonment for that offence or with a fine related to the offence or both in some cases.

Both the Information Technology Act, 2000 as well as Amendment Act, 2008 have set three authorities for settlement of civil disputes-

- Controller of Certifying Authorities,
- Adjudicating Officer, and
- Presiding Officer of the Cyber Regulations Appellate Tribunal

Affected parties need to seek compensation up to rupees one crore from the person who committed the violation. One could approach the Adjudicating Officer as per Section 46 by filing a complaint. The adjudicating officer is quasi-judicial authority as he needs to hold a proper enquiry before stating a decision. It should be noted that as per Gazette notification for Information Technology Rules, 2003, the important provisions for Scope and Manner of holding inquiry are-

- to exercise jurisdiction for contraventions in relation to Chapter IX of the Act;
- to receive all complaint from the complainant;
- to issue notices along with all the documents to all the necessary parties to the proceedings, fixing a date and time for further proceedings;
- to hold a proper enquiry or dismiss the matter or may get the matter investigated;

- to fix a schedule for production of documents (including electronic records) or evidence; and
- to hear and decide every application, as far as possible, in four months ideally and the whole matter in six months.

When the adjudicating officer stands convinced of the case and believe that it falls under Chapter XI of the Act requiring punishment besides a fine, then he will transfer case to the Magistrate who has powers to judge the case. The complete role of Cyber Regulations Appellate Tribunal comes after the adjudicating officer completes the task. Since the Cyber Regulations Appellate Tribunal is an appellate body, it can examine the legality of the order passed by adjudicating officer under IT Act or controller of certifying authorities. Any person who wishes to appeal an order passed by the lower bodies can go to Cyber Regulations Appellate Tribunal for grievance redressal. If the person is not satisfied with order of Cyber Regulations Appellate Tribunal, he/she can go and appeal to the Higher courts within 60 days of the order.

The IT Act is considered as a law providing data protection regime to ecommerce and e-governance sectors. Some of those chapters are considered as the foundation for data protection in India. The Act does not state anything about direct marketing. It does not have any provisions for people to opt out of direct marketing. There is no legislation that deals with direct marketing per se. Few years back the Supreme Court has asked banks etc to maintain a 'do not call' registry for the benefit of data subject. Now a data subjects gets rights to opt out of online consumer databases.

3.2 The Financial Institutions Act of 1993

This Act gives a framework to India's tradition of maintaining confidentiality in bank transactions. In India the bankers have an obligation to maintain secrecy of bank account. The account of the customer in the books of the bank records all his financial dealings and depicts the true state of his financial position. If any third party can get free access to such records it could lead to undesirable consequences. The banker is therefore under an obligation to take utmost care in keeping secrecy.

Thus, the banker cannot disclose any information regarding his customer's accounts to any third party and the banker must ensure that all necessary safeguards are taken to prevent any data leak. In the case of Kattabomman Transport Corporation Ltd. v. State

Bank of Travancore and others, [29] it was held that among the duties of the banker towards the customer is the duty of utmost secrecy, which arises out of the trust factor in banker customer relationship. It may be noted that the duty of the banker to maintain secrecy is not an absolute one, there are some exceptions, when the law requires such disclosures to be made or when the practices and usages permit such disclosure.

3.3 The Indian Telegraph Act

Wiretapping is regulated by the Telegraph Act of 1885. Since there were numerous phone taps scandals, the Supreme Court defined wiretaps as "serious invasion of an individual's privacy". The Indian Telegraph Act of 1885 under article 5 allows authorities to intercept messages for surveillance. According to this Act, power is levied on the government to take control of licensed telegraphs and to order interception of messages in the cases where:

1. On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government, or any officer specially authorized in this behalf by the Central Government or a State Government, may, if satisfied that it is necessary or expedient so to do, take temporary possession (for so long as the public emergency exists or the interest of the public safety requires the taking of such action) of any telegraph established, maintained or worked by any person licensed under this Act.
2. On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government consider that necessary or expedient so to do in the best interests of the sovereignty and integrity of India, friendly relations with foreign states or public order or for preventing any outrage to the commission of an offence, for reasons to be recorded in writing, by order, direct that any particular message or messages between people related to a particular topic , transmitted by telegraph shall be intercepted or detained and may be disclosed to the government. It should be duly noted that any press messages intended to be published in India of correspondents accredited by Central Government or a State Government will never be intercepted or detained, unless their transmission has been prohibited under this sub-section.

[29] AIR 1992 Ker.351.

As per section 7(2)(b), the Government may prescribe standard rules and necessary precautions to ensure that there is no improper interception or disclosure of messages, but it has been seen in the PUCL v Union of India 1996 Case that no such rules have been enacted by the Government at that time. However, with reference to wiretapping by the government, the Supreme Court has laid proper and specific guidelines defining who can tap phones and under what circumstances:

- Only the Union Home Secretary, or his counterpart in the States, can issue an order for a tap;
- The government must completely prove that this is the only mean to obtain the sought information;
- The Court has duly mandated the development of a high-level committee to review the legality of each wiretap.[30]

3.4 CREDIT INFORMATION COMPANIES (REGULATION) ACT, 2005

Passed in May 2005, the Credit Information Companies (Regulation) Act was notified in the official Gazette on June 23, 2005. It was passed to regulate credit information companies and to provide provisions for "information privacy principles and furnishing of credit information". The Act was mainly formulated to ensure that there is an efficient distribution for credit information and other matters concerning it. Under this a credit information company is defined as a company registered under the Companies Act, 1956 (1 of 1956) and has been duly granted registration certificate under section (2) of Section 5.Here credit information is defined as data relating to–

- the amounts and the types of loans or advances, amounts outstanding under credit cards and other credit facilities granted or to be granted, by a financial institution to any borrower;
- also the kind of security taken or proposed to be taken by a financial institution from any borrower against credit facilities granted or proposed to be granted to him;
- or the guarantee furnished, or any other non-fund based facility granted or proposed to be granted by a credit institution for any of its borrowers;
- the creditworthiness indicators of any borrower of a credit institution;

[30] *Privacy & Human Rights, « An international survey of privacy laws and developments », Electronic Privacy Information Center, 2004*

- any other matter which the RBI may, consider necessary as part of credit information to be collected and maintained by credit information companies.

According to this Act, Credit institution has been defined as primarily a banking company and includes corresponding new bank, the State Bank of India, a subsidiary bank, a co-operative bank, the National Bank and regional rural bank; a non-banking financial company; a public financial institution; the financial corporation established by a State; the housing finance institution; and also includes the companies engaged in the business of credit cards and other similar cards and companies dealing with distribution of credit in any other manner.

The concept of personal data according to this act is "information of an identifiable individual but it does not include name, business title/address, or telephone number. This definition bears a lot of resemblance with the European definition of personal data. As per this Act, all credit information companies must ensure that all information they get are properly recorded, collated and processed by the credit institution. Under this Act, "collector" means a credit institution, or a credit information company, as the case may be, which collects credit information in of a borrower. The main provisions of the Act are-

3.4.1 Section 19 Accuracy and security of credit information

A credit information company or credit institution or specified user is a company which has accumulated credit information should take all precautions to ensure the data maintained by them is accurate, complete, duly protected against any loss or unauthorized access or unauthorized disclosure thereof. The data should be accurate at all times as it directly affects the data subject.

3.4.2 Section 20 Privacy Principles

As per Section 20 (b), all Credit Information Institutions or Credit Information Company needs to adequately specify why information is collected and how it will eventually be used. They should restrict disclosures to a minimum level. Both company and specified user need to have obligation of furnishing correct information to such a body.

Section 20(c) duty bounds every credit institution, Credit Information Company and specified user to check accuracy of credit information before furnishing this information. This Section imposes a duty of accuracy on these institutions.

Section 20(d) states principles regarding the proper preservation of data maintained by credit information company, credit institution, and specified user. Also principles for period for which such information may be maintained, manner of deletion of such information and maintenance of records of credit information are provided under this section.

As per Section 20(f), Reserve Bank may have certain regulations having principles and procedures related to credit information. Such principles are-

1. Care in Collection of Credit Information

All credit information companies need to be sure that all information they collect/receive are-

- Accurately recorded, collated and processed;
- Safeguarded against loss;
- Is protected against illegal access, use, modification or disclosure.

All credit institution companies must update information every month and needs to take steps to supply update, accurate, complete, correct and current information to the Credit Information Companies.

2. Data Security and Secrecy:-

Credit information companies, the credit institutions and the specified users must at all times establish security and other relevant procedures as per the rules under the Act. The core principles for employees are-

- The credit information company's employees need to sign a confidentiality agreement.
- The credit institution and the specified users need to form procedures for authorizing their employees to handle all credit information. Also, this information needs to be transmitted via a secure medium.

3. Access and Modification:-

Credit information companies and credit institutions need to establish proper procedures in order to allow a person to access his own records. The person must make a request must prove its identity. A right to modification is also included in this principle-

- The credit information company should correct, add or alter the data as the case may be within 15 days of getting the request from credit information company or specified user.
- The credit institution must have established procedure, to get a modification request from a person requesting such information. Credit institution should inform and notify to credit information company within 30 days of original request.

4. Data Collection Limitation:-

The principle covers proportionality as seen in European directive. It requires that data collected by credit information companies needs to be accurate and relevant to fit the purpose of why it is collected. This is exactly as per European standards.

5. Data Use Limitation:-

According to this principle, the permissible purposes for which the credit information companies take available credit information reports may be as follows-

- To comply with court, tribunal, etc orders
- As per the request of borrower other than individual for credit information pertaining to itself against payment of processing fees.
- As per the request of an individual for credit information pertaining to himself against payment of a nominal fee (not exceeding Rs 100) and on identifying himself.

6. Data Accuracy:-

As per this law, credit information company needs to take all steps to ensure that data is completely accurate and complete. The credit institution is responsible for correctness and complete accuracy of data submitted to credit information company and should update data monthly. Specified users must ensure that they are using correct information at all times, so they make correct decisions in respect to giving credit.

7. Archiving/Length of Preservation:-

Credit information company will retain and collect all information for minimum of 7 years. There are different provisions for information relating to criminal offences and information related to financial defaults and civil offences (data should be removed from the history after 7 years from the date of first reporting). Any information about non-individuals will be of permanent nature.

3.4.3 Section 21 Alteration Of Credit Information Files And Credit Reports

The right to access will be of the person who seeks to grant credit facility. Request will be done by credit institution. Access right is limited to only credit information.
The right to rectification will be granted to clients or borrowers when they request that their information should be updated. Updating the information can be done by making the relevant correction or addition in data.

Credit Information Company should apply safeguards falling under the rule of the Act. Credit Information Company must make all employees sign a secrecy and loyalty declaration. Such institutions should ensure clear procedures for authorizing employees to exercise this information only on a need to know basis. The medium through which all data is collected and transmitted should be safe and secure. Section 19 states that an individual can file a complaint with the RBI against a credit information company, credit institution for acting against the Act. The Reserve Bank is empowered to impose penalty or reprimand Credit Information Company, credit institution or specified user having contravened the Act.

3.5 INDIAN CONTRACT ACT, 1872

The Indian Contract Act, is another solution to protect data. Contract as a term includes all types of contracts like partnership, agency, contracts of carriage etc. When there is nothing specific mentioned on data protection corporates rely on this Act. Due to scale of operations, corporates have several contracts with many other corporates and agencies who are involved in collection and storage of data along with the subsequent protection of the same. Contracts like ‘non-circumvention and non-disclosure’ contract, ‘user license’ contract, ‘referral partner’ contract etc are entered by them. These contain important clauses like arbitration, confidentiality, privacy etc.

Contracts like these assist in smooth and continued running of business. BPO companies go a step further and implement processes like BS 7799 and the ISO 17799 standards of information security management which tends to restrict the amount of data at disposal with employees. There are contracts made between, Indian 'data importers' with 'data exporters' in other countries. Such contracts are abide by Indian Law and it fulfils the requirement of the overseas customers. As per this law, whenever a person commits any breach of contract, the other party will receive compensation for loss suffered or alternatively in exceptional cases court may demand for 'specific performance' of the contract against party in default.

3.6 SPECIFIC RELIEF ACT, 1963

The Specific Relief Act is aimed at giving adequate remedy to the one whose right is infringed. It gives punitive relief in the form of temporary and perpetual injunctions (sections 37 and 38) to the plaintiff to avoid any further breach of obligation existing in his favour. A person can pursue case against any service provider as ask for injunction against it if such service provider has not fulfilled the contractual obligations done between them. The court is in a position to order the service provider from the assertion of a right, or from the commission of an act, which would be contrary to the rights of the plaintiff. Further, the plaintiff in a suit for perpetual injunction as per section 38, or mandatory injunction under section 39, may also choose to claim damages either in addition to, or in lieu for, such injunction and the court may, if it thinks fit, award such damages.

3.7 INDIAN PENAL CODE

The single provision that deals with Data Protection under Indian Penal Code is section 406 and it imparts punishment for Criminal Breach of Trust. Section 406 states that an individual who chooses to commit a criminal breach of trust shall be punished with imprisonment which may extend to three years, or with fine, or with both. There is another section parallel under Indian Penal Code which can be levied upon person responsible for data theft is section 420. Section 420 tends to deal with any kind of cheating or fraud committed by a person and data theft can be considered as a kind of cheating committed by the service provider for data entrusted to them by customers. Punishment provided under this section is imprisonment which may extend to 7 years

and a fine. However, Indian Penal Code has fully failed to incorporate punishment for crimes related to data which are quite prevalent today. Since India became a leading market in outsourcing, and processing data from globally for companies this has become critical.

3.8 COPY RIGHT ACT, 2012

The Copy Right Act protects all kinds of literary work and as per section 2 (o) "literary work" will also include computer programmes, tables and compilations including computer data bases.

3.9 THE RIGHT TO PRIVACY BILL, 2011

Right to Privacy Bill, was introduced in February 2011 at the Rajya Sabha by Rajiv Chandrashekhar. The Bill aims to provide adequate security to privacy of life including those who are in public life. It gives a broader perspective to data protection. It may be noted that such Privacy Rights are not absolute as there are some privacy breaches are permitted in the Bill itself. As per this act there are some changes in the government interception mechanism. The modification is with done in the view of several safeguards which are put into place to avoid unauthorised and unnecessary tapping orders. According to this Act, Data Protection Authority of India will be established to regulate the data processing, collection, etc from people at large. The body will supervise all private parties which are engaged in the collection and storage of personal data.

The Right To Privacy Bill incorporates the protection for the storage, collection, processing and use of data which includes personal information, sensitive personal data, interception of communication, surveillance photographs, fingerprints, body samples, DNA samples, health information, etc. As far as privacy rights are concerned in India they essentially are a mere set of procedural safeguards. Safeguards ensure stronger privacy right.

3.9.1 Index: Constituents Of The Bill

The Bill contains fifteen chapters and ninety-four sections and has been divided in the following manner:

Chapter	Section	Name
I	1 – 2	Preliminary
II	3	Right to Privacy
III	4 – 13	Privacy of Communication and Prohibition from its Interception
IV	14 – 23	Procedure for Interception of Communication
V	24	Prohibition of Surveillance and its Regulation
VI	25 – 26	Use of Photographs, Fingerprints, Body samples of persons, DNA samples, and other samples taken at Police Station
VII	27 – 28	Health Information Privacy
VIII	29 – 31	Privacy relating to Data
IX	32 – 42	Obligation and Procedure for collecting or processing or using or disclosing data
X	43 – 48	Residuary
XI	49 – 62	The Data Protection Authority of India
XII	63 – 66	Grants, Funds, Accounts and Audit and Annual Report
XIII	67	Settlement of Disputes
XIV	68 – 84	Offences and Penalties
XV	85 – 94	Miscellaneous

The Right to Privacy Bill, 2010 legislation can be identified as follows:

- Giving statutory Privacy Right to the Citizen of India.
- Establishing the Data Protection Authority.
- Ensuring there is efficient monitoring and regulatory mechanism.
- Mandating responsibilities on the data processor
- Establishing a Dispute settlement body

3.9.2 Providing A Statutory Privacy Right To The Citizen Of India.

Section 3 (2) of the Right to Privacy Bill 2011 gives an inclusive definition of Right to Privacy which is divided into 12 categories given as below:

a) Confidentiality of communication
b) Confidentiality of private/ family life
c) Safeguarding of honour and good name
d) Adequate protection from search, detention, or exposure of lawful communication between and among individuals.
e) Complete Privacy from surveillance
f) Total Confidentiality of banking and financial transactions
g) Total Confidentiality of medical and legal information
h) Comprehensive protection from identity theft (criminal, financial, identity cloning, medical)
i) Protection from use of photographs, fingerprints, DNA samples, and other samples taken at police stations or other places
j) Protection of data relating to an individual.

The term right to privacy pass across several areas such as privacy of core communications, bodily/physical privacy, confidentiality, and privacy of records and data protection. The comprehensive definition of right to privacy also includes "confidentiality of communication, family life, bank and health records, protection of honour and good name and protection from use of any kind of photographs, fingerprints, DNA samples and other samples taken at various points such as police stations and other places for legitimate reasons." Unlike Right to Information Act, this section is broad and does not restrict right to privacy only to claims against the state.

3.9.3 Providing The Data Protection Authority.

Data Protection Authority shall be established by the Central Government of India as per Section 49 of the Right to Privacy Bill. This will help in order to regulate and maintain the data storage and data processing. The Data Protection Authority is headquartered in New Delhi and shall consist of chairperson, and not more than two other members. The Chairperson and the other members as per procedure are to be appointed by the Central Government. Section 50 of the Bill provides list of qualifications of the Chairperson along with the other members which is, the chairperson and the other members shall possess special knowledge of, and relevant professional experience diverse fields, data protection, finance, law, management and consumer affairs. This will enable them to adopt a multi-disciplinary approach to data

protection.

Section 52 is concerned with the powers entrusted to the Chairperson. The Chairperson of the Data Protection Authority will be having complete powers of general superintendence and direction in the conduct of the affairs of the Authority and besides this presiding over the meetings of the Authority. The Chairperson as part of his/her duties will also exercise and discharge such powers and functions of the authority and adequately discharge any other powers as may be prescribed over time.

3.9.4.Providing An Efficient Monitoring And Regulatory Mechanism.

This Bill aims to provide establishment of an oversight body that is "Data Protection Authority of India" which will further investigate any other complaints related to breach of data protection. The main functions of this body are,-

- to monitor development in data processing and computer technology;
- to review law and to evaluate its effect on data protection
- to give appropriate recommendations and to receive representations from members of the public on any matters related to data protection.
- to investigate data security breach and issue complete orders to safeguard the security interests of affected individuals whose personal data is likely to have been compromised by such breach.

3.9.5.Imposing Responsibilities On The Data Processor

A data processor should always ensure following two things for processing a data:

a) Purpose for which data has been obtained
b) Whether it has been obtained in a legal manner.

All data processor who collect, process, disclose or use data of an individual are duty bound to ensure that all data used by him or his agents is complete, correct, accurate and updated and remains so for the duration that it is under their custody. For sensitive data, the person who is assigned to collect, process, disclose or use such data of any individual will obtain written consent of such individual and where such individual is minor their such consent shall be obtained from his parents or legal guardian.

3.9.6. Providing A Dispute Settlement Body.

Any aggrieved person can make an application to Cyber Appellate Tribunal set up under the IT Act 2008 for adequate resolution of dispute arising between an individual and data collector. Any person can by decision or order of an authority shall appeal to the Appellate Tribunal, within the period of thirty days from the date on which copy of such order, decision or direction is received by the individual. The Tribunal as part of the process will hear both the parties for the dispute. The copy of every final order passed in the application or appeal shall be send to both the parties by the Tribunal. The Appellate Tribunal needs to adequately check legality of dispute and ask for the records relevant to disposing of such application or appeal and make decision based on that.

3.9.7. *Scope Of Right To Privacy*

Section 3(1) of the Bill states that, all individuals are entitled to right to privacy and same are subject to the law for the time being in force or an order of court. Any privacy right as part of the Privacy Bill is not absolute and is subject to existing laws in force. Hence any law in contravention of Privacy under Section 3 has preference and legal validity. Numerous laws are excluded from the privacy right under Section 90. Though these laws would have been exempt as per Sec. 3(1), no chances have been left by excluding statutes and pivotal rights such as the Right to Information Act; The Prevention of Corruption Act; under the privacy rights. Section 89 of the Bill makes space for a wide array of rights to be included in the scope of the statutory right of privacy, which may be present.

Section 3(2) gives an inclusive definition of Privacy by providing for 12 kinds of manifestations of privacy, which are listed below:

a) Confidentiality of communication
b) Confidentiality of private/ family life
c) Safeguarding of honour and good name
d) Adequate protection from search, detention, or exposure of lawful communication between and among individuals.
e) Complete Privacy from surveillance
f) Total Confidentiality of banking and financial transactions
g) Total Confidentiality of medical and legal information
h) Comprehensive protection from identity theft (criminal, financial, identity

cloning, medical)

i) Protection from use of photographs, fingerprints, DNA samples, and other samples taken at police stations or other places

j) Protection of data relating to an individual.

3.9.8. *Privacy Of Communication And Interception*

The Bill further provides for confidentiality of all relevant communications and safeguards as stated in Chapters III and IV of the Bill. The term interception has been defined broadly as "undertaking the stopping of transmission of any communication, or interception or detention thereof (including tapping of the telephone conversation or copying of data)" Likewise, "confidentiality" is defined as the thorough process of sharing facts, ideas, opinions, thoughts, and information through speech, writing, gestures, sound, images, signals or pictures, graphs, symbols, diagrams between two or more individuals through telephonic conversations, radio messages, electronic mode (including internet or satellite) or postal letter or any other mode". The primary interception safeguards are as below-

1. Section 4 mandates that every citizen of India is granted right for having his/her communication protected from interception. Like other rights, this is also not an absolute right and is limited by the provisions of the Bill under discussion. Moreover, there are two clauses to intercept a communication legally.

- All conditions under Section 5(2) of the Indian Telegraph Act, 1885 must be satisfied.
- An order for interception must be issued by an officer not below the rank of Home Secretary [Ministry of Home Affairs, Government of India] and the Home Secretaries of the State Governments which records the satisfaction of these conditions.

This provision is relevant to all kinds of surveillance. It goes beyond and also applies to ancillary activities to interception. An exception is created with respect to the authorities that can make such an order, and it is stated quite clearly that this power can be delegated to another officer of a stipulated rank due to its sensitive nature. Further, in emergency situation (the kinds have been specified) interception can be made without an order under Section 5 after obtaining subsidiary approvals from the Central and the State governments (stipulated officers).

2. As per Section 6(2), the approval giving authorities have a limit of 3 working days to place the order before an appropriate authority and get confirmation. The authority should send a confirmation within 7 working days maximum. If no confirmation is received, then the interceptions need to be compulsorily discontinued and any further interception will require permission of the Union Home Ministry or the State Home Secretary, as the case maybe.

3. As per the Bill two bodies are primarily established. One is the Requisitioning Service Agency (Government) and the other is the Service Provider (the Telecommunications Company). Both bodies are mandated to appoint nodal officers (not ranking below Superintendent of Police or Additional Superintendent of Police in case of government and two senior executives in case of service provider) and the relevant transaction of exchange of any information collected shall occur only between them, since the matter is confidential and of a very sensitive nature. Strict guidelines are put in place while exchange of such data to ensure monitoring in case of any data leaks.

4. Service Providers have been placed with Provider responsibility, and they have a timeline of fifteen days to submit a list of authorizations, to the Security agencies to verify and confirm authenticity of the directions received by them. Further, stipulations are provided with respect to secrecy, maintenance of data, destruction of records etc.

3.9.9. *Prohibition Of Surveillance*

It should be noted that people are not allowed to undertake surveillance, either by following a person physically or closed circuit television etc to -

- Explicitly identify an individual, who is a citizen of India and monitor personal details and consecutively reveal his private information in public
- Affect their right to privacy amounting to civil wrong.

It should be well noted that in case of public emergency, public safety or for prevention and detention of crime the state government with the authorization of the Central Government is permitted to use all data collected through surveillance.

3.9.10. Changes To Noticed If The Bill Is Passed

If the Privacy Bill 2011 gets passed in Parliament there will be changes relating to current data protection procedures. Such changes will be as follows-

- The bill restricts complete interception of communications and allows only certain cases with prior approval of Secretary-level officer not below the rank of home secretary at the Central level and home secretaries in state governments
- Compulsory destruction of intercepted material by the service provider within two months of completing the interception.
- Establishing a Central Communication Interception Review Committee to review all interception orders passed.
- Central Communication Interception Review Committee is empowered to order destruction of material intercepted under the Telegraph Act.
- Illegal interception is punishable with a maximum of five years' imprisonment, or a fine of Rs 1 lakh, or both, for each such interception. Therefore, it becomes a cognizable, non-bailable offense.
- Complete disclosure of legally intercepted communication by "government officials, employees of service providers and other persons" is punishable with imprisonment up to three years or fine of Rs. 50,000 or both. It is ambiguous if it is a cognizable offence or not.
- A surveillance done against section 24 of the bill will result in 5 years imprisonment or fine up to Rs. 1 lakh or both for each surveillance.
- Getting personal information on False Pretention from any person or officer of the government by impersonation will lead to punishment of such a person with the fine of Rs. 5 lakh.
- Any officer or Employee of the Service Provider or the Government who knowingly discloses information which is restricted under this bill, to anyone not entitled to know the same will fully be liable for the offence punishable with the fine of Rs. 5 lakh according to the Bill.
- Collecting and using of photographs, fingerprints, DNA samples in public of any citizen of India shall make such person liable for the imprisonment of up to 5 years or fine of Rs. 1 lakh or both.
- Any person who acquires data illegally(intentionally and without authorisation from Data Subject or Data Controller) will be liable for the fine from 7 lakhs to 10 lakhs

3.9.11. *Probable Effects Of The New Bill*

For Employers :

Employers are mandated to establish a privacy policy and obtain the consent of the employees to the privacy policy in writing. The employer has to give the employee the right not to provide Sensitive Personal Data. The privacy policy needs to fully state that what information is being collected, and how it will be used for and the name and disclosure on the contact details of agencies collecting this data. There are rights for an employee to access all information about him, to rectify the information and to require the information to be deleted.

For Multinationals in India :

Multinationals are required to maintain centralized databases of information about their businesses globally, including, information about employees, service providers and customers. As per regulations laid down under the Bill it is observed that in some parts it more conservative than even the European rules. Overseas companies who receive the information will have to establish processes to comply with the rules. Indian entity will need to necessarily have requirements for having a privacy policy, consent for collection, disclosure about purpose of use of the information and who will be collecting the information and total consent from the providers for providing such information to outsiders.

For The Outsourcing Industry :

These refer to business dealing with information or Sensitive Personal Data in India have to comply with the rules set by the Right to Privacy Bill, even if such information is not concerning citizens of India. The vendor in India or his customer overseas will need to be compliant with requirements of the law for concerned individual, such as the consent for collection, notification obligations, right of access, correction and withdrawal.

Applicability To Financial Information :

The Bill covers banking and financial information of an individual generally within the provisions for safeguards of Privacy Right. The inclusion of financial information sets a high standard of privacy protection relating to information that is received in the

ordinary course of business especially by financial institutions which is very confidential in nature.

Consent As A Condition :

The requirement of seeking consent is a mandatory condition for the use of all sensitive personal data. Under European law consent is just one ground on the basis of which sensitive personal data can be used which is contrary to the Bill. For example, for personal information generally, (including financial information), one can process such information without consent of the provider if it is necessary for performance of a contract with the provider of the information eg banks processing customer details as part of ordinary business.

Security Standards :

The data controller shall take appropriate measures to ensure safeguard of the data. Such security measures are taken to prevent:

- loss, theft, damage, unauthorised destruction of data,
- illegal processing of data,
- unauthorised disclosure whether accidental or intentional of data.

Data controller has to take due care while engaging sub-contractor to process the data on his behalf. Data Controller is duty bound to ensure that the contract arrangements made between them is maintained properly.

Overseas Transfer Of Personal Data From India :

Personal Information of an individual cannot be transferred to a country outside India unless that country ensures an adequate level of safeguards for the protection of personal data according to the Bill.

3.9.12. *REMEDIES PRESCRIBED UNDER THE BILL*

The Bill recognizes all kinds of privacy rights. Hence, it also provides remedies in case of breach. The following are remedies that can be claimed by an aggrieved person.

a) Compensation

As per Section 76, any person who suffers damage can claim for compensation. One can claim for damage caused to him by any data controller in accordance with section 76.

The damage caused needs to be due to any contravention on part of the data controller. These penalties are in the form of fines. They are intended to restrict illegal conduct. Section 76 is aimed to compensate the loss suffered by a person.

b) Civil Remedies

Section 84 states that the individual, whose right to privacy has been adversely affected, may bring a civil suit against such persons who have caused such violation. This is addition to any criminal proceedings existing against such person (violator).

c) Criminal Remedies

Chapter XIV provides for various offences that may be committed against the right provided for under this Bill. As per Section 82, Court may take cognizance of offence under this Bill, based on complaints made by the authority.

3.9.13. Limitations Of The Bill

Usage of electronic recording devices in public is an important and expansive aspect of privacy, which is yet to be directly covered by Indian law. The Bill covers the basic usage of electronic devices with built-in cameras, and defines any violation done as a personal violation. The Bill has taken a disciplinary approach, making it criminal to take photographs in situations contrary to the laid-out regulations, rather than protective in nature, i.e., working to protect individuals from harassment and blackmail, etc. So we can say the Bill is lopsided.

The Bill does not include scenarios such as Google street view, satellite photographs, news channels, and live feeds at events and conferences. In such cases live data is being transmitted and posted on the Web for public to watch. Privacy interests of the photographs taken in public by media are different than those which are under personal control. Photographs taken in public by media are substantive and are directly engaged with freedom of expression. For example, in matters such as freedom of expression encompasses both those of the photographers and journalists producing material for his/her journal. Law needs to develop with emergence of new age technologies.

As per Section 30, under following circumstances activities do not constitute

infringement if privacy rights:

- sovereignty, integrity and security of India, strategic, scientific or economic interest of the State.
- preventing incitement to the commission of any offence
- avoiding public disorder or detection of crime
- in the best interests of friendly relations with foreign states
- in connection with the publication by any person of any journalistic, literary or artistic material.

As per these exemptions perhaps "Right to Information" is not completely clarified hence its interpretation is also discretionary. Any person who has his right to information can use the data and still cannot be held liable for misuse of data is left with a vague answer. Even "Preventing incitement" is too broad as a term and is most likely to be misused. "Prevention of public order" is also bound to get misused and this can be extended to all cases of politically motivated issues. Publication by any mode as part of journalism is also exempted from infringement of privacy rights unless it get proven in court that such publishing is of material which is reasonably expected to be held private. This perhaps can be identified with "Freedom of Press" which is also a vague version.

The Bill appears to indicate a single representative office of the Data Protection Authority with all the administrative responsibilities. For settlement of disputes, the Cyber Appellate Tribunal (CAT) established under ITA 2008, has the responsibility of being first trial court for all complaints between a data subject and the data controller. As of now there is a single CAT in Delhi which is not sufficient to meeting the requirements of ITA 2008.India needs a number of Cyber Appellate tribunals or their Benches to be established in many State capitals so that victims can access them in proximity to their place of living and there should only be nominal charges for it.

4. Conclusion

The main concern of companies is to cut cost by outsourcing part of their activities to third countries where the workforce is cheaper. India has a leading position in this sector. As per the National Association of Software and Service Companies (NASSCOM), the main reasons behind India's success in the outsourcing industry are:

- Abundant, skilled, English-speaking manpower. India is one of the largest English speaking countries in the world, which is important for the development of the call centres.
- Young and educated population. The highest number of available graduates in India was also a major advantage in 2001. The educational system has a good general level and emphasizes on mathematics and science which contributes to a better understanding of the computers. Private schools tend to offer specialisation in diverse programming skills and computer language courses are encouraged by the Government. This leads to a big man force available to work in this sector.
- A gradual improvement in telecom and other infrastructures which are to be par with global standards. India had no software industry historically, but investments in brand new technologies were made possible allowing for a better specialisation and the development of new technologies that were not yet company-owned. In this regard, outsourcing has been an optimum way to cut costs and to improve overall services in comparison with the prospects offered by their own enterprises.
- Strong quality alignment among players and their overall focus on measuring and monitoring quality targets.
- Quick turnaround times and the ability to offer 24x7 services based on the country's inherently unique geographic location that allows for leveraging time zone differences.
- Proactive and positive business environment policy which encourages ITES/BPO investments and simplifies rules and procedures. A relatively friendly tax structure, which places the ITES/BPO industry on par with IT services companies.
- The government is well aware of the opportunities offered by the outsourcing business, has fostered their growth by creating Software Technology Parks and allowing relevant tax exemptions on all exports and duty-free hardware imports.

The outsourcing business is of primary importance for the Indian economy: The ITES-BPO industry generated total revenues of US$ 3.9 billion in 2003-04, representing a growth of around 45.3 percent over the previous year. The sector was expected to reach revenues of around US$ 5.7 billion by the end of 2004-05, at a growth rate of 44.4 percent.[31] Regardless of this India, in its immediate surroundings has a bigger problem

[31] Indian ITES-BPO Trends (2003-04), available on www.nasscom.org/artdisplay.asp?cat_id=800

to deal with, which is the bad reputation outsourcing has earned overseas. Many foreign corporations decided not to outsource their activities.

However, companies who are focusses on cost rationalization will probably continue to outsource to India, and we shall propose attractive incentives and protection against potential obstacles in order to favour the outsourcing sector. Comprehensive data protection legislation will be helpful in India. American and European consumers are worried about data security. [32] There have been cases of data thefts (credit cards numbers, etc.) in banks etc which have highlighted the high risk of outsourcing in countries which do not have the legislature for data protection legislation and also the enforcement capabilities.

To dissuade consumer fears, some American States considered of banning the outsourcing of data concerning particular domains (such as medical, financial or personal information). The overall thorough compliance with European standards would facilitate outsourcing from Europe and reassure Western consumers on the European market as well as other partners. Due to tight global competition, with the emergence of the West Balkan countries and China as major players, India has with time relentless will in setting up the best legal and economic environment possible, and quality infrastructures to keep attracting foreign companies to its shores. The economic importance of the outsourcing business in India must certainly be taken in account given the dangers of misuse of quantity of processed data and risk it could lead for data-subjects.

[32] "An outbreak of data protectionism?", The economist, September 2nd 2004, available on www.economist.com. visited on 21st October 2014.

CHAPTER 5

COMPARING INDIA'S LAW RELATING TO DATA PROTECTION WITH LAWS AT USA AND EUROPEAN COUNTRIES

Table Of Contents

1. INTRODUCTION

The term "data protection" has become a collective need for numerous nations globally. New age technologies have made it possible for third party access or theft of anyone's non-public personal information, which has made governments vigilant in their efforts to enact or improve legislation on data protection. There are many cultural differences among nations which thereby lead to various differences in the regulatory models for privacy protection. India is not a completely private nation. Indian culture favours extended family living concept, which has average of 5 persons per house in India. American culture is more influenced by concept of individuality. As per the 2000 U.S. Census, 26% of all U.S.A, homes were single-person house, which although far behind Sweden at 46%, was nevertheless enormously greater than that of India where the single-person households are scarcely seen. Since India is a collectivist society, Indians usually have more trust in others, and therefore result there is more trust in those on people provides personal information.

In India, personal and non-personal information is distributed freely and without thinking twice of any ramifications of it. Public dispersion of personal information has inherently become a method of indicating the translucent functioning of the government. Numerous agencies of the government collect both personal and non-personal data; this data is consecutively stored in silos and each agency of the government maintains the information using diverse fields and formats. Government databases do not interact and since they are not organized uniformly, the information that gets collected by different departments cannot be merged.

India has gradually developed as a market leader in outsourcing and processing data from all over the world. India has played a vital role in the management of the millennium bug where there was a huge chunk of the work which was outsourced in India. India had begun to appear as a leading country in the computer industry. In late 1990s, the software market was booming in the US, and a lot of companies outsourced their software needs to India. India was the leading source and host of data outsourcing and data processing due to the big progress of the IT and BPO (Business Process Outsourcing) sector which had the infrastructure and procedures in place to handle and

access sensitive, personal and non-personal information. Indian employees have a lot of personal and non-personal information of clients of global corporations.

There were reports of data theft in these sectors when in June 2005. The Sun newspaper claimed that one of its journalists could purchase personal details including passwords, addresses and passport data from a Delhi IT worker for only £4.25 each, thereby exposing India's lack of data security mechanisms. [1] Other instances were also noticed for BPO frauds in India such as New York-based Citibank accounts being looted from a BPO in Pune and a call centre employee in Bangalore selling credit card numbers to fraudsters who stole a big amount of USD $398,000 from bank accounts in UK. The news was fake but still it raised critical doubts about data protection in India. Since there is vast volume of data available with such industries in India from other countries which have stringent data protection laws, there is therefore an overall rising awareness for complete protection of data in India through international treaties.[2]

Since data protection is well known area of law nowadays driven mainly by the need to address data protection concerns in a highly technological era, India till date doesn't have dedicated data protection legislation. Data protection is mainly governed by the contractual relationship between the parties, and the parties are fundamentally free and can enter into contracts to determine their relationship defining their own terms of personal data, sensitive data, data which is restricted to be moved out of or to India and mode of handling of the same. These contracts do not serve as effective remedy for breach of data security. However, getting into contractual obligations with parties is bit difficult and time consuming.[3]

---

[1] Danish Jamil & , Muhammad Numan Ali Khan, Data Protection Act in India with Compared to the European Union Countries, International Journal of Electrical & Computer Sciences IJECS-IJENS Vol: 11 No: 06, Available at: www.ijens.org,

[2] Vidushpat Singhania, Is there a database right protection in India? Lakshmikumaran & Sridharan Attorneys, Available at: www.lakshmisri.com, visited on 13th October 2016.

[3] Arun Agarwal, Need for data protection law, The Hindu, 24th May 2005, www.hindu.com, published on 24th May 2005

As per reports, India controls approximately more than 40% of the global outsourcing market of software and back-office services. U.S. companies form largest part of clients of the BPO industry. So, cross-border transfers of information in form of data from other countries, into India have raised questions about the ability of Indian companies to have proper safeguard in place to protect this information. Indian employees tend to have large access to data of personal and non-personal information about customers of multinational corporations. Processes like transcribing medical records, credit card applications and bills, handling of mortgage loan applications, and reviewing of insurance claims are tasks associated with the BPO sector etc.

Member countries of the European Union and Canada have stringent laws that ensure protective measures are followed for all with the cross-border transfer of information belonging to their citizens. U.S. companies are also required to comply with industry-specific laws enacted by the U.S. Congress along with state laws, which regulate the use and transfer of customer's information. Additionally, multinational U.S. companies need to provide adequate safeguards, as prescribed by the European Union, or obtain EU (European Union) Safe Harbour designation, whenever they perform any cross-border transfer of the data of citizens of EU countries.

Doubts are raised on the capability of Indian companies to safeguard when sensitive information is transferred to India under BPO contracts. India till date does not have any protective legislation for data, even though the Indian Ministry of Information Technology and the National Association of Software and Service Companies (NASSCOM), two pivotal players in India's BPO industry tried putting efforts. In 2004, both agencies drafted a data protection law which ultimately resulted in rectification of the Information Technology Act, which is not comprehensive and lacks protections for sensitive personal information. India also has no agency which is equivalent to the U.S. Federal Trade Commission to issue and enforce compliance of data privacy rules.[4]

[4] "Offshore Outsourcing to India by U.S. and E.U. Companies," Barbara Crutchfield George and Deborah Roach Gaut, 6 U.C. Davis Bus. L.J.. 13 (2006).

Neither the U.S. nor the Indian constitution fundamentally recognizes a right to privacy. The case law of both countries has acknowledged a right to privacy which is indirectly derived from constitutional rights to free speech and other such rights. Both countries depend majorly upon self-regulatory efforts taken by industry lobbies to protect personal information. Unlike India, the U.S. has enacted various laws for some industries providing protection to certain types of personal data.

The Indian companies mainly function in absence of any basic specific legal or regulatory requirements related to information collected in the form of data, unless any compliance is required by contract. Under contractual data protections, the degree of protections varies from company to company and client to client. Though Indian companies have undertaken full security safeguards still, other internal problems can fundamentally influence total efficiency of such precautionary measures. Corruption in the corporate sector remains to be apparent problem in India, which ultimately affects the level of confidence by foreign companies in Indian BPOs.

India has a close bond with countries globally which has deepened in recent years. India from aid donor and recipient has gradually turned to one of partnership which gives immense growth opportunities for mutual benefit. India is the largest source provider in outsourcing and data processing owing to growth of the IT (Information Technology) and BPO sector which handles critical and sensitive, personal and non-personal information of people around the world. India does not enjoy general data protection statute. Nevertheless, the judiciary has derived a "right of privacy" which is available under Articles 19(1) (a) (the fundamental right which grants freedom of speech and expression to citizens of India) and 21 (the right to life and personal liberty) of Indian Constitution. All cases that govern right to privacy are decided in the context of Government actions which results in private citizens being denied their overall right to personal privacy. The privacy judgment has given private citizens a right of action to contest against any breach of privacy by another private citizen. Data protection and personal privacy jurisprudence in the country is not yet fully developed at par with other nations.

2. ***Present Scenario for Data Protection in Various Fields***

2.1 Data Protection at Educational Institution

India has neither any law nor any rules for protection of student. The researcher has extended the area of research to educational institutions like pre-schools. Here the sample selected by the researcher was the principal of pre-schools at Ahmedabad and Vadodara. Five pre-schools from each city were selected involving random sampling method. To be more specific five pre-schools from the satellite area of Ahmedabad and five per-schools from the manjalpur area of Vadodara were selected for carrying the research. Schools easily share their records of students with the school's affiliated concerns. The researcher has carried her research from schools across Ahmedabad and Vadodara. As survey carried by researcher reveals that many pre-schools share their record of students enrolled in their pre-school with the high-school they are affiliated with. For example, at Vadodara the affiliated school of euro kids is Vibgyor, and euro-kids share their details of the students along with the registered mobile number (one of the personal data) of the parents with the affiliated schools without the consent or knowledge of the parents. Vibgyor in order to promote their school use the direct marketing strategy and approach the parents of students enrolled at Euro Kids. However, the researcher also found that such pre-schools does not share their student data with any other inquiry i.e., if any person inquire about the details of some students he is not related to, then such person is denied any kind of information as this is the policy of the pre-schools. Moreover, infringement of the rules laid down in the policy does not lead to a major offence or punishment.

The researcher further inquired about the pictures of the students used in advertisement of such school. Every school uses pictures of their students for major or minor promotional advertisement of the school; however, no consent oral or written is taken either from the student or from the parents of such student before using their pictures. When inquired about the same with the parents a mix review came up, some parents liked that their kid's pictures were selected for the promotional activity while some were not so happy with it but, at the same time took no action against it as there is nothing as a remedy for such act. The school too doesn't follow any procedure for selection of such pictures, the one who looks good in the pictures are the criteria for

selection. The researcher further came to know that taking consent from the parents of the students for using their kid's pictures was not felt necessary by school in-charge.

Unlike India, US and EU gives much more importance to the protection of their student's rights. Under EU laws an educational institution can be any public or private agency or institution which is the recipient of funds under any applicable government program. It is mandatory for the educational institution to obtain written consent from a parent, guardian or eligible student before releasing education records or personally identifiable information contained therein to any individual, agency or organization. Even a written consent is taken from the parents or guardians before using the student's picture for any kind of promotional activity of school. USA on the other hand has enacted Family Educational Rights and Privacy Act (FERPA) with the aim to protect the student's educational records which is applicable to all educational institutions that receives funding from U.S department of education. According to FERPA it is mandatory for the educational institution to obtain written consent from a parent, guardian or eligible student before releasing education records or personally identifiable information contained therein to any individual, agency or organization.

The Draft Bill suggested by the researcher address these issues by providing consent clause in the Act and also the Right to be Informed clause by the data manager can curb the above discussed issues.

2.2 Data Protection and Internet with Children under the age of 13.

The law in US and EU restricts children below 13 years to access social media sites. However, US has gone a bit further where a website operator before collecting a child's personal information must notify the child's parent of its data collection practices and must obtain parental consent to collect the information. After the written consent of the parents such website operator can collect the data of a child and process it for the purpose he has collected such data.

Unlike these countries, there is no law in India which restricts child below the age of 13 to explore the world of social media. The researcher herself tried to create an

account on Facebook a very famous social media where she entered her age which was below 13 years but she was denied. However, there are chances that the child enters a wrong birth date and is allowed to have an account at Facebook. The researcher has come across many Facebook account where it can made be out from the photographs that the children holding such account are below the age of 13 years. Parental control over the computer or laptop is the only option available to the parents of such child who holds account at the social media website.

EU has not implemented a separate law for the protection for child below 13 years of age; however Data Protection Directives extends its protection to any kind of data collected. USA has moved a bit further for the safety of children below 13 years of age by enacting the Children's Online Privacy Protection Act (COPPA)[5]. The motto behind COPPA is of protecting children below 13 years of age in their use of the Internet by regulating how websites collect, use, and disclose children's personal information. Under COPPA, before a website operator who collects a child's personal information must notify the child's parent of its data collection practices and must obtain parental consent to collect the information.

2.3 Data Protection at Hospitals

In India there are many hospitals like private clinics, multi-speciality hospitals, etc. Here the question of data related to health arises. Hospitals carry large amount of data of their patients, in other words hospitals are the holder of health data of their patients. The researcher carried her research at the multi-speciality as well as private hospitals. The sample selected by the researcher was HR of multispecialty hospitals at Udaipur and Ahmedabad. Three hospitals of Ahmedabad and two hospitals of Udaipur were selected by the researcher. Multi-speciality hospitals generally follow the trend of having its own policies and rules which restricts sharing of information about their patients. Moreover, such policies once again lack strict enforcement and therefore are not followed efficiently. Furthermore, the information of the patients is shared with the relative of such patient or the person who has accompanied such patient, but if an unknown person inquires about the details of any patients then such person is not shared

[5] 15 U.S.C. §§ 6501, *available at* www.coppa.org, visited on 27th March 2015.

with any kind of information. Many times bribing a peon or ward boy can make the leakage of information. Majorly no hospitals follow contract or agreement of confidentiality with their employees, thus confidentiality part runs on ethics and trust on the employees of the hospital. Indian culture plays important part here, as Indians easily share their personal information with others. Hence, due to this reasons the hospitals do not sign and contract or agreement for confidentiality of data with their employees.

The scenario at private clinics is different, for example at a maternity home the details of patients are easily shared with others (persons who are not related to the patients). Many maternity homes share the information of their patients with the Stem Cell Preservation Centre. The Stem Cell Preservation Centre after acquiring details about the patients enrolled at the clinic calls such patients as part of direct marketing for their services. The researcher inquired with the people who receive such calls, many of them do not opt for stem cell preservation and many gets harassed by such calls but are left without remedy as this is normal course followed at almost every clinic. No consent of the data subject is taken by the private clinic before sharing their information with others.

Another, important information that the researcher gathered is that the advertisement given by the Hospitals as their promotional activities involve pictures of many patients. Here the concern is that the consent of patient is not taken before using their picture for promotional activities. Moreover, the HR themselves were unaware that such an act can be considered as infringement of privacy. However, in India using pictures without consent for promotional activity is a common practice used by almost everyone involved in business.

Such practices are not followed at US and EU as there is no easy flow of data to the person not concerned. Importance to privacy is at much higher level at USA and EU. The data controller needs to take consent of the data subject before sharing his information. The data controller even informs the details of third party to which the data is to be transferred and the purpose of the data is to be transferred.

2.4 Data Protection at Service Providing Companies

There are many services providing companies that functions now a days. These service providers majorly includes online service providers, for example, Sulekha.com, various digital box provider for TV, etc., these companies also hold large amount of data. Such companies promote their service through calls, mails and Short Message Service (SMS) and the approach is direct without taking consent of the subject. The researcher examined such service providing companies and came to know that only Sulekha.com takes consent of the subject before approaching them. If a person once called sulekha.com for any service assistance, the sulekha team sends sms to such person for taking his consent for whatever options he opts i.e., call, sms or mail from sulekha.com. Thereafter unlike other service providing companies Sulekha.com never approaches such person again unless the person himself approaches sulekha.com for any other assistance.

However, in EU countries and USA consent method is followed. Any company while providing its service to the customer asks for his written consent for the further promotional communication. Moreover, people in Europe are far more reserved and therefore they take don't provide their consent and are not disturbed by such companies. While in USA people are not as reserved as Europe but at the same time are not open as Indians hence, if consent given such customers are approached for the promotional activities of the company. Moreover, the consent of the customer is given importance and the companies act accordingly. If a customer does not provide his consent then such customer is never approached for the things he never consented.

2.5 Data Protection at Banks

Banks are the most crucial place where secrecy if not maintained can lead to disaster. Banks hold a large amount of vital information about the financial data of the person having account at that the bank. Financial information is the most crucial information that banks carry. Banks handles the money transactions, monetary balance, lockers, etc of their customers. Banks whether it is nationalised bank or private bank follows the guidelines of Reserve Bank Of India (RBI), the Banking Law of India and along with that each bank has its own rules and regulations circulars which are updated from time to time. Banks never share the details of their customers to any other person.

In case of banks unlike hospitals even the family members are not shared with the details that bank holds about their customer. There is no employer and employee contract or agreement practice followed at the bank, once again confidentiality part relies on ethics and trust amongst the employees of the bank.

However, when it comes to marketing even banks doesn't leave the game; they use the data of their customer and call, message or mail them for their promotional schemes relating to credit and debit card, international credit card, etc. While carrying the research the researcher came across the information that, certain banks have appointed a personal banker for every customer having account balance of Rs. 1 lakh and more. The appointment of customer relation officer is done suo moto by the bank and the data subject never asked for his consent for such service. Such personal banker personally calls the customer and informs about various investment schemes of the bank depending upon the balance of money available at the customer's account. Hence, it's clear that the financial records as well as other personal details like mobile number, address, name, etc of the customer are known by the personal banker.

The researcher also came across the information while carrying on her research that, some banks hires private call centres on contract basis for their assistance. The hired call centres are shared with the information of the customers of such banks. Customers while having any query with such bank calls at its toll free number or service centre and such toll free or service centre calls are diverted to the private call centres. No data subject is asked to consent or is informed about transfer of their data to the third party. Hence, information of many customers has been leaked. The researcher herself was a victim of a fake call, which said that

"the person who is calling is calling on behalf of SBI bank and instructs the call receiver to provide with the debit card number as well as PIN (Personal Identification Number) so that they can secure it."

When such call receiver provides the PIN number their account is hacked. Many people are trapped in such fake call and have lost their money. The fake calls increased at an extreme rate that SBI took a step and called their customer just to inform them not to provide with any information about the credit or debit card or any other information regarding the customer's bank account. The same call from SBI bank was received by

the researcher. SBI has to telecast advertisement for many times on the national television channels making their customer aware about not sharing their OTP (One Time Password) or PIN to any person calling from bank. This situation is result of the absence of any data protection laws in India. The third party whom the bank hires leaks the data of customer and without any stringent law such acts are increasing day by day.

The above discussed issues are been taken care by the consent clause inserted in the Draft Bill suggested by the researcher. The transfer of data to third party is also taken care under the Right To Be Informed clause of the Draft Bill. It might happen that the Data Protection Law prevents the checking of credit worthiness of the data subject which is important for the assessment to made of the customer before granting him any kind of loan or grants by the banks. Hence, this issue needs to be taken care of while drafting the law. An explicit provision for companies checking for credit worthiness has been incorporated in the suggested Draft Bill.

When compared to other countries, USA has enacted the Gramm-Leach-Bliley Act (GLBA)[6] imparts the duty over the financial institution such as bank to respect the privacy of their consumer and ensure security along with confidentiality of that consumer's non-public personal information. In USA and EU no such practices are followed. Consent of the data subject is taken before approaching them for any promotional schemes of the bank. When the customer intends to seek information about investment schemes of the bank only then they are provided with such information. The laws for data protection are stringent and therefore no fake call frauds take place in these countries.

2.6 Data Protection at Outsourcing Business in India

The outsourcing business is of first importance for the Indian economy: The ITES-BPO (Information Technology Enabled Services-Business Process Outsourcing) industry generated total revenues of US$ 3.9 billion in 2003-04, representing a growth of around 45.3 percent over the previous year. The sector was expected to reach revenues of around US$ 5.7 billion by the end of 2004-05, at a growth rate of 44.4

[6] 20 USC § 6801 available at www.gpo.gov, visited on 12th June 2017.

percent.[7] Regardless of these promising perspectives, India in its immediate surroundings has a problem to tackle: namely the bad reputation outsourcing has earned abroad. Consequently, under public pressure, foreign public authorities decided not to outsource their activities. The foremost question challenging data protection in India had come up from outsourcing business.

The data protection at the call centres are governed by the contracts both the parties undergo. When it comes to national call centres, firstly the data subject is not informed about their data being processed and when such data is being transferred to third party the consent of data subject is not taken. Talking about the international call centres the scenario is different.

The India BPOs follows the guidelines published by ISO (International Organisation for Standardization). The ISO from time to time upgrades its guidelines and is followed by the BPOs across India. During the research it was revealed to the researcher that the international call centres across India followed the guidelines of ISO. However, the ISO provides mere guidelines which are not binding over the companies. It is upon the company authority's decision to follow the ISO and even how much to implement from the guidelines given. Hence, as it is just guidelines there is no effective redressal for the offences.

Apart from the ISO guidelines and in absence of any legislative framework for data protection in India, the BPO industry needs a kind of self –certification for achieving the same results. In order to implement this, various industry verticals would need to appoint independent certifying agencies to prescribe data standards and to overlook compliance with data protection principles. The system is voluntary but relies on peer pressure to ensure that conscientious corporations remain compliant with their obligations in order to continue to be accepted by their customers and business eco-system. Some companies in order to build confidence amongst the client they receive data from, appoints certifying agencies from the countries they receive data which turns to be very costly for the companies.

[7] Indian ITES-BPO Trends (2003-04), available on www.nasscom.org, visited on 19th November 2017.

While this self-certification does offer a lighter touch, it does not give the individuals, whose data is at risk, any form of legal remedy in case of a breach of their personal privacy by the self-certifying organizations. In such situation of any organization commits a data breach, the individual whose data has been lost will have no legal recourse. Data protection can only be ensured under a formal legal system that prescribes the rights of the individuals and the remedies available against the organization that breaches these rights. It is imperative, if the aim is to create a regime where data is protected in this country, that a clear legislation is drafted that spells out the nature of the rights available to individuals and the consequences that an organization will suffer if it breaches these rights.

Along with the self-certification method, in order to provide assurances of privacy protection of non-public personal information and other data the BPO collects from its foreign clients, many BPO service providers in India have engaged in self-regulation, in recognition of the damage that could be inflicted on the Indian BPO industry resulting from major security abuses. Those self-regulation results in stringent security measures that have been developed and recommended to BPO service providers, such as the following:

2.6.1 Key Information, such as passwords, is encrypted and unseen by employees.

The data in BPOs are stored at computers. To ensure the data protection, the company has to set up software with the help of which employees can never know the passwords of the computers at their workplace. Such passwords are important to start up the computer or the devices employees are using. Hence, with the restriction over the passwords the company saves data it is processing and thus ensuring safety of the data flowing into their company. Such software are available in market and the company due to absence of any law relating to data protection has to buy such software, which is a kind of extra expense to the company.

2.6.2 Special training sessions are conducted for the employees relating to data protection.

At the time of joining BPO the company arranges for special training programs for their employees. This program includes an entire session for data protection. Here the employees are made aware about the importance of data which flows to their company and at the same time protection terms and conditions of such data is been discussed. The employees are also thought about the personal and non-personal data as well as sensitive personal data. The employees are also made conscious about the responsibility the company is carrying for the protection of such data. The clause of confidentiality of the contract made between the employer and employee for the data protection is also made clear at this session. Also the consequences arising out of the breach of such contract by the employees are being made understood to the employees at these training sessions.

2.6.3 Employees are monitored via closed-circuit television i.e., CCTV.

Closed Circuit Televisions (CCTV) are installed at proper place at the company in order to monitor the activities of the employees. The CCTV is placed in such a manner that a person can notice even the computer screen of the employees. A supervisor is appointed for close monitoring of the employees and if the employ behave in a doubtful manner actions are being taken against him. This is done in order to secure the data flow to that company majority of which is from out of India.

2.6.4 Entry is restricted by requiring microchip-embedded swipe cards.

Employees are provided with microchip swipe cards with their identity. Scanning or swiping such card keeps check on the entry and exit of the employees as well as it assures the company that none other than the employees are entering into the premises of the company. At many companies even thumb impression scanner are installed to keep the entry and exit of the employees more secure. This restriction ensures that no other people except the employees of that particular company are entering the sensitive premises or work area of that company. Visitors to the employees are provided with other card so that even the entry and exit of the visitors can also be closely monitored.

2.6.5 The mobile phones of the employees are also prohibited in the work area.

Mobiles are the latest gadget available to a person. Mobile can easily transfer information in fraction of seconds. Even clicking a photo can make the action of theft easy for a person. Hence, to avoid such circumstances, all the BPO companies restrict mobile phone at the work area of their employees. The employees need to surrender their respective mobile at the lockers provided by the company before entering into their work area. In case of emergency from the family or other relative, the employee can be contacted at the company's telephone number where an operator has been appointed and the employee is been called to the place where the operator is present for the communication.

2.6.6 Even bags, briefcases and other belongings of the employees are prohibited in the work area.

The employees are allowed only with the swipe cards and other essentials into the work area. In case of male employee bags or briefcase they carry along with them are not allowed at the work area and in case of female even the purse is restricted at the work area. Every employee is provided with lockers which are outside the work area of the employee. Such lockers are utilized for keeping bags, mobile phones and other unnecessary belongings of the employees. Such lockers can be accessed by the employees at the break time or in some case they require during their work hours. The position of such lockers is important as it is kept outside the work area of the employee there is no loophole left that the employees can get themselves involved in the data theft activity.

2.6.7 Armed guards posted outside offices i.e.; physical security system.

Guards are posted outside the company. Armed guards are posted outside the main gate of the company for the security of the whole company but on top of that physical security i.e., guards are posted even internally at the company. For example, QX international company is a BPO working at GNFC tower, Ahmedabad. QX company has acquired 6 floors of the GNFC tower and at every floor security guards are posted who seats at the entry and exit point of the employees. These guards ensures that every person entering into the work area of the company scan, swipe or punch as the case may

be the card provided by the company for the entry and exit. Such guards provide temporary cards to the visitors only at the instructions and permission of their superiors. Hence, this assures the company that no person enters the work place without the knowledge of the responsible person.

2.6.8 Change of Identity of the Employee.

The researcher while carrying out this research came to know that whole identity of the employee is changed at BPO. Approximately 90% of the international BPO companies changes the identity of their employees. For example, the name of employee of QX International is MRUNAL JOSHI, this identity is changed by ROY ANDERSON, and this is done just to secure that the data. A person would never know that Roy Anderson is dealing with data flowing to QX international company as Roy Anderson is actually Mrunal Joshi once he steps out of the company. Other reason for the change of identity is that any employee of such BPOs cannot be located even on various social media website.

2.6.9 The non-accessible e-mail ids provided to the employees.

Every BPO provides their employees with the email id created by the company. Such email id created by the companies remains accessible only at the work area and not from any other computer outside the work area.[8] Hence, this ensures that the data employees are processing at the company is not shared or accessed from any other place. This also helps the company secure the data flowing from outside India and thus ensures the data giving company about the security and safety of their data.[9]

Many data theft incidents are being heard frequently these thefts are possible due to absence of data protection legislation. Thus when the researcher asked about having data protection legislation for India, International Call Centres agreed to it with 100% of the ratio while the national call centres came up with 40 % ratio for agreement.

[8] Information gathered by carrying out research through interviews and questionnaire.

[9] Information gathered by carrying out research through interviews and questionnaire.

2.7 Data Protection and Direct Marketing

Direct marketing is the much used mode of marketing in today's time. Every company whether it is selling a product or a service provider are involved in direct marketing for the promotion of their product or service. Even Banks, educational institutions, tuition classes, mobile companies, online shopping companies, etc are using direct marketing for the promotion of their product and services. Now a day even small shops, restaurants, salons, etc are also using direct marketing to approach their target audience. Direct marketing is considered to be the best way of marketing to leave an impression on the target audience. Hence, all the companies use direct marketing in one or the other way for the promotion of their product or service. Direct marketing involves a direct approach to the target audience. This approach includes tele-marketing, send SMS or mailing to the target audience.

As the market grows marketing methods also grows and the frequency of marketing also increases. Earlier the best way of marketing was either publishing the product or service in the local/national newspaper, promoting it on television channels and lastly was mouth to mouth promotion. Now a days the options for approaching a person has increased. A person can be approached through a phone call, short message service, what's app and e-mails. These are usual way to approach a person directly. India is faced with a new phenomenon-telemarketing. This is facilitated, to a large extent, by the widespread use of mobile telephones. Telemarketing executives, now said to be available for as low as US $70 per month process information about individuals for direct marketing.[10] This interrupts the peace of an individual and conduct of work. There is a violation of privacy caused by such calls who, on behalf of banks, mobile phone companies, financial institutions etc. offer various schemes. The right to privacy has been read into Article 21, Constitution of India, but this has not afforded enough protection. A PIL against several banks and mobile phone service providers is pending

[10] Does India need a separate data protection law?, available at www.knspartners.com/files/BNA%20Article-180106.pdf

before the Supreme Court alleging inter alia that the right to privacy has been infringed.[11]

It is said that "Anything beyond limitation creates nuisance, even eating beyond limitation causes damage to one's health". Hence, direct marketing today may be the best way to approach target audience, but from the target audience point of view the scene may be different. Direct marketing has increased to that extent that DO NOT DISTURB (DND) kind of services has to be activated. The researcher went to the common people specially educated to get the answer that whether the direct marketing is helpful or is a nuisance.

The results of the survey conducted by the researcher were that 70% of the public thought that direct marketing is a nuisance to them. The people involved in direct marketing calls their target audience at any time hence, it creates nuisance for the people. Many people have opted for DND services but 30% of those people say that it is ineffective. Even though such people have registered with the DND service, they still receive marketing calls from different companies. Even banks uses tele-marketing method for giving away different types of loans, credit and debit cards etc, and the record they use is the data of their customer who are account holder of that bank. When asked about the consent method used in the foreign countries 90% of the people agreed to it. According to Consent method the company ask the person about making them know for the promotional scheme company is coming up with, if the person opt for the same only then he is being disturbed otherwise no calls, SMS or e-mails are send to such person.

The EC Directive confers certain rights on the people and this includes the right to prevent processing for direct marketing.[12] Thus, a data controller is required not to process information about individuals for direct marketing if an individual asks them

[11] Mr. X v. Hospital Z, (1998) 8 SCC 296. "The right to privacy is enshrined in Article 21 of the Constitution of India".

[12] Directive 95/46/EC 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, Art. 14.

not to. So individuals have the right to stop unwanted marketing offers. It would be highly beneficial that data protection law in India also includes such a right to prevent unsolicited marketing offers and protect the privacy of the people.

2.8 Data Protection at Tele-communication (Mobile) Service Companies

There are many mobile service providing companies operating in India. Any person who wants a sim card needs to provide authentic residential proof like licence, Aadhaar card, etc. at the tele-communication service company. Such tele-communication service companies have their call centres to deal with queries of their customers, any other assistance to the customers and marketing of their own company. Companies like Vodafone, Idea, Airtel and Reliance have their own call centres.

The researcher also came to know during her research that may mobile service providing company hires a private call centre for resolving the issues of their customers and such private call centres are provided with the personal data of the customer without his consent or knowledge. Hence the data of the customers are handled by many other including the company they are providing with their authentic documents. Today direct marketing is the easiest way to approach people and the tele-communication companies use this mode of marketing to promote their services. While carrying on the survey the researcher came to know that person having a Subscriber Identity Module (SIM) card of Vodafone gets contacted by the Idea Company for their promotional marketing information. This is possible only when there is leakage of data from one company to another.

The worst situation arise when the data of the data subject is leaked and such data subject is messaged through sms by any other company that such data subject's number is selected in a lucky draw and is eligible of 1 million dollars or so. The data subject is trapped in such act ultimately loses his money behind getting such prize. Many such cases are heard very often in the news-paper or news channels. Many companies hire private call centres and no contract of confidentiality is signed by such companies with the hired company. Even the data subject is not informed about the transfer of their data to the third party and the purpose of the transfer of the data. Many people at Dakor

village of Gujarat received calls from Afghanistan at mid-night and if they answer such call their mobile account balance is being deducted or emptied. When approached to the company there was no solution for the mobile account balance with the company.

The researcher herself had travelled to Sweden (one of the country of EU). There the researcher took a SIM card at Sweden. The company of researcher's husband provided with the authentic documents after which researcher got her SIM card. While giving the sim card a form was attached to it, which was a consent form provided by the tele-communication service company. The form was about whether the customer is interested in getting any promotional marketing calls, sms or e-mails (all of them or either of them) from the company. The researcher opted '**NO'** for this and for the next four months no sms, calls or e-mails were send to the researcher by the tele-communication service company. Such is the practice followed at EU and USA.

The Draft Bill suggested by the researcher has a clause incorporated that the data subject has a Right To Be Informed by the data manager about which of their data is being processed and if it is to be transferred to third party prior consent of the data subject is mandatory.

2.9 Data Protection at Insurance Companies.

Insurance companies as banks carry vital information of the customer. There are many insurance companies getting people as well as things insured across India. People get themselves insured for various purposes. There are many types of insurance like life insurance, medical insurance, car insurance, two wheeler insurance, etc. Insurance companies heir agents for people to get insured. Out of all these types of insurance Life insurance is an important one as it deals with person's death and the sum insured after his death. Life insurance insures that the nominee of such insured person gets money after the accidental or un-natural death of such insured person.

The researcher approached agents of insurance company to carry on her survey. During the research the researcher came to know that the insurance agent do not share the information of their customer with other by himself. However, if someone (relative of insured person) approaches him for the information then the agent may provide

information of the insured person. For example, if Shivani Joshi has taken life insurance of Rs. 500,000 from some insurance company and husband of Shivani Joshi approaches the agent for the information of her insurance the agent would provide the details of it without informing or taking consent from Shivani Joshi. There is no contract or agreement of confidentiality undergone by the insurance company and the insurance agent.

There are chances that the agent gives the personal information of the customer to others also. While answering the question of the researcher the agent of Life Insurance Corporation Of India (LIC) said that the family members of an insured person can know the details of insurance as there is no harm in sharing the information to the relative. The family members are often shared with the insurance details of the insurance subject; this is due to the influence of the cultural set up in India. However, the agent further said that if the insured person himself instructs the agent not to share his information with others then the agent would deny. Moreover, here the data subject needs to approach the agent for not sharing his information rather than the agent approaching the data subject for the consent, which is the normal practice followed at EU and USA.

Hence, this issue has been taken care in the Draft Bill suggested by the research through the clause of taking consent before transferring the personal information to the third party as well as keeping the onus of confidentiality over the data managers (which can be insurance agents also).

2.10 Data Protection In The Opinion Of Common Public

The target respondents amongst common public were from the age of 25 to 65. Approximately 150 questionnaires were distributed amongst common public across Ahmedabad and Vadodara to have an idea about the how important data protection is considered by them. The researcher has used random sampling method, and the public selected worked in different fields like house wives, business person, teacher, free lancers, employees of advertising companies, lawyers, and so on. The researcher has not confined to one particular class of people for sampling. The subject of the research is such that the researcher had to select educated public so that they can intellectually answer the question addressed in the questionnaire. 60% of the sample selected for common public was unaware of any law that can protect their privacy or data. While

70% of the public agreed having data protection law if it can help them get away from the direct marketing methods of advertising. 30% of the public opined that genuine data protection law must be implemented in India so that they can have a clear vision for what is being done with their data. The specific concern here was the people are unaware about the source who provides their contact details to such direct marketers, and for that reason they need to know what is done with their data. When explained about consent method used by countries having data protection laws 100% of the public agreed on inserting the clause of consent if the Bill is being framed for data protection. The overall outcome from the questionnaire distributed amongst common public was that they were treating direct marketing as a nuisance and if a law can cut off their nuisance every sample wished to have such law. Thus the Draft Bill suggested by the researcher has an explicit provision for direct marketing. The Bill has also incorporated a provision of right to be informed granted to the data subject according to which, the data managers has to inform about what and how the data is processed to the data subject.

2.11 Data Protection at Pathology Laboratory

Pathology laboratory collects the blood samples of the patients from which DNA can be extracted (DNA is a part of sensitive personal data). Hence, the researcher extended her research area and included pathology laboratory also as it was important for the subject matter of the research. The researcher carried out her research at the pathology laboratory across satellite area Ahmedabad city. Pathology Laboratories are those places where we go for our blood check-ups or body profile, etc. The pathology laboratory collects blood samples of the people who opt there for diagnosis of their blood. The laboratory based on the analysis of the blood prepares report of such patient and provide the report. These laboratories are huge centre of DNA samples of many different people coming there for test. Such laboratories provide home service too i.e., they go to patient's home to collect samples and sometimes even deliver their report at home. The researcher carried on her research for inquiring about the samples they collect. The researcher came to know that such pathology laboratory provides report to any person who comes with the payment receipt of the patient without verifying anything about the person. When the researcher inquired about the samples the lab collect they said that such samples are disposed of after the test is carried on. Moreover,

the maximum quantity of the samples they collect are used for the test to be conducted, hence may be a very less quantity or sometimes nothing are left out of samples after carrying out the test of the samples. The records of the patients are not kept with the laboratory until asked to save. If the patients ask to save it then only the records are saved.

3. AADHAAR Card Concerns the Data Protection in India

Aadhaar Card has become important after the act of demonetization and PM Narendra Modi urging citizens of India, to enrol for the UIDAI programme. The data for Aadhaar Card is collected by "Unique Identification Authority of India (UIDAI)" which is the nodal agency and is directly governed by central government of India, and such data stored into central database. PM Modi is trying to employ Aadhaar as the main link to monitor all transactions and eventually take all transactions online.

3.1 Issues Making Aadhaar Card Inevitable for Indians

Contrary to the statement of non-compulsion for enrolment of Aadhaar Card made by the government, the government itself makes Aadhaar automatically compulsory for the citizens of India in many areas. Following are the aspects for making Aadhaar enrolment compulsory for the citizens of India:

- Citizen who enrolls for government exams needs Aadhaar Card for enrolment according to the rules of the governing body of such exam.
- Withdrawing money from of Provident Fund (PF) of the citizen also needs Aadhaar Card without which receiving PF is not possible.
- School admissions form must be submitted with the Aadhaar Card of the student which is taken as identity and residential proof.
- Even mobile numbers need to be linked with the Aadhaar Card.
- Under privileged citizens who get government subsidized benefits such as getting food grains at subsidized rates, building houses and toilets for which government helps financially, etc, all such activities needs Aadhaar Card
- Post demonetization, depositing money amounting more than 50,000 rupees in the bank account needs to be submitted with Aadhaar Card as per the government rule.

- The gas cylinder registration is also linked with Aadhaar Card for keeping an eye on the people getting subsidized rated gas for their home.
- Tickets for the IPL match were sold to only those who provided Aadhaar Card. [13]
- AIIMS waived off registration fees for those who have Aadhaar Card.[14]

3.2 Security Concerns relating to Aadhaar Number

Aadhaar Cards are equivalent to Social Security Number for the citizens of India. However, the government needs to address the following threats due to Aadhaar Card:-

- Increase in data collection will also expand the chances of identity theft and data leaks.
- No separate Data Protection Legislation is enforced in India so Indians are left with limited options for the redressal of their identity theft or data leaks.
- To accomplish Aadhaar project, the government has employed private agencies hence, now all those private agencies have records of citizens from the area they had been allotted for collection of data.
- Aadhaar Card project involves nearly all the banks, mobile service providing company, agencies duly appointed for the distribution of gas on demand by the citizens, schools, colleges, electricity connection centres and government departments listed as registered users with the access of the data of Aadhaar making the data collected risky. Aadhaar data leak is easy for all those who have collected data.
- Storing data collected for Aadhaar at central database might create various kinds of problems for public at large as well as the government.
- Finding of personal details becomes easier. Hence this will be unsafe in terms of identity theft. It is a double edged sword.

[13] Want To Buy An IPL Ticket? Better Have An Aadhaar Card! Article by Hemanth Kashyap published in India Times on January 29, 2017, available at www.indiatimes.com.

[14] No Aadhaar? pay Rs. 100 for registration at AIIMS article at The Hindu, available at www.thehindu.com,

- Since bank accounts are linked with the Aadhaar Card, bank transaction or ATM cum Debit cum Credit cards use will give opportunity for many miscreants to misuse it.
- Frauds relating to ATM have become common and with the link of Aadhaar Card to the bank account the risk increases.

3.3 Comparison of Aadhaar Card with Social Security Number

Aadhaar number under UID scheme is available to all residents of India. [15] Social security number is mainly for citizens in USA however the Department of Homeland Security may grant it to some non-citizens working there.[16]

3.3.1 Governing Legislation:

Aadhaar was formulated by the Planning Commission of India. The UIDAI was created as subset office under the Planning Commission in 2009. [17] Aadhaar Act got enacted which primarily governs the protection of UID (Unique Identification Number). Most portions of the Information Technology Act 2008 apply to the UID scheme, section 43A and associated Rules (India's data protection standards) which do not apply to the UIDAI as the provision has limited jurisdiction only over body corporate. The SSN (Social Security Number) is very different from the UID Scheme. SSN is primarily governed under Federal legislation, but the issuance, collection, and use of the SSN is governed by both Federal and State legislation particularly the Social Security Act 1935[18] – this inherently gives legal backing to it. The Privacy Act 1974, also regulates the collection, access and sharing of the SSN by parallel Federal Executive agencies.[19]

[15] Aapka Aadhaar. Available at: uidai.gov.in. visited on 26th February 2018.

[16] Social Security Numbers for Noncitizens. Available at: www.ssa.gov, visited on 24th June 2018.

[17] Government of India Planning Commission "Notification". Available at: uidai.gov.in, visited on 24th June 2018.

[18] The Social Security Act of 1935. Available at: www.ssa.gov, visited on 24th June 2018.

[19] The United States Department of Justice, "Overview of the Privacy Act of 1974". Available at: www.justice.gov, visited on 23rd April 2018.

3.3.2 Purpose:

Aadhaar is primarily a biometric based authenticator and also a single unique proof of identity**.** The Aadhaar number is usually used as a single proof of identity and address for Indian residents that can be used to authenticate the identity of an individual in transactions with organizations that have adopted the number. The UID scheme is a mechanism for reducing fraud in the public distribution system and enabling the government to better deliver public benefits. [20] SSN is primarily a record keeping scheme for all government services. SSN was initially formulated to track an individual's earning in the Social Security System. [21] In 1943 via an executive order, the number was adopted in all Federal agencies. In 1977 it was the Carter administration stated that explained the number could represent a means to validate the status of an individual (for example if he or she could legally work in the country) however it was not supposed to serve as a national identity document. The SSN primarily tracks individuals in the social security system and as one form of identification amongst different corporates. The SSN card does not independently serve as a proof of identity.[22]

3.3.3 Storage, Process, Access and Disclosure

Aadhaar data is generated via number of sources through which it is collected and stored at CIDR (Central ID Repository) which happens to be UIDAI's data centre, via an online mechanism. Data after being processed in the Data Warehouse using Business Intelligence tools is then converted into forms that can be accessed and shared easily. The process is bit ambiguous and does not state whether the organizations that authenticate individuals through Aadhaar number store the number at organizational level. Biometrics is considered as sensitive personal information in accordance with Information Technology Act and hence is strictly safeguarded.[23]

[20] UID FAQ: Aadhaar Features, Eligibility. Available at: resident.uidai.net.in/faqs

[21] History of SSA 1993 - 2000. Chapter 6: Program Integrity. Available at: www.ssa.gov, visited on 23rd April 2018.

[22] Social Security Number Chronology. Available at: www.ssa.gov, visited on 23rd April 2018.

[23] Information Technology (Reasonable security practices and procedures and sensitive personal data or information rules 2011) available at: deity.gov.in,

3.3.4 Utility:

The Aadhaar number is universal in nature and can be adopted by any public or private entity as a single means of identifying an individual. The UIDAI has explicitly stated that the Aadhaar number is not mandatory, [24] and the Supreme Court of India has at its end also clarified that services should never be denied on the grounds that an individual does not possess an Aadhaar number. [25] With reference to SSN public and private entities can request the SSN to track individuals in a system or as a form of identifying an individual. Any private business can for legitimate reasons request and use the SSN as long as the use does not violate federal or state law. An individual can refuse to provide their SSN, but a private business can if it wishes to deny a service on these grounds. [26] Any public authority requesting the SSN must always provide a disclosure notice to the individual explaining if the provision of SSN is mandatory or optional. As per the Privacy Act of 1974, no individual can be denied a government service or benefit for not providing the SSN unless Federal law categorically requires the number for a service.[27]

3.3.5Verification:

If an organization, department, or platform has adopted the Aadhaar number as a form of authentication, they can choose to send it for verification to the UIDAI. The UIDAI will respond with a yes or no answer. While using their Aadhaar number for personal authentication individuals can submit their number and demographic information or their number and biometrics for verification. [28]

The requests for SSN verification will be responded by SSA only in following circumstances:

[24] Aapka Aadhaar. Available at: uidai.gov.in, visited on 23rd April 2018.

[25]Business Standard, "Aadhaar not mandatory to claim any state benefit, says Supreme Court" March 17th, 2015. Available at: www.business-standard.com.

[26]SSA FAQ " Can I refuse to give my social security number to a private business?" Available at:faq.ssa.gov, visited on 12th August 2018.

[27]The United States Department of Justice, "Overview of the Privacy Act of 1974". Available at: www.justice.gov, visited on 12th August 2018.

[28]Aapka Aadhaar. Available at: uidai.gov.in, visited on 12th August 2018.

a) SSA will definitely verify that the name and the number match as per the records, before issuing a replacement SSN.
b) When legally authorized, the SSA verification system will verify SSNs for government agencies.
c) When legally permitted the verification system of SSA will verify a worker's SSN for pre-registered and approved private employers.
d) Also, if an individual has given his/her consent; the SSA will verify a SSN request from a third party.

While verifying SSN's sent for verification, the system will automatically responds with either confirmation that the information matches or that it does not match.[29]

3.3.6 Replacement of Number:

If an individual has lost their Aadhaar number, they can regain it by following a replacement process. However, even when UIDAI fails to locate such number re-enrolment for new Aadhaar number is the only option left for such individual.[30] The UIDAI has built the Aadhaar scheme with such understanding that the biometrics are a unique identifier and biometrics cannot be lost or stolen, hence have not explored a system to address the possibility of stolen or fraudulent use of biometrics. While, if an individual loses his/her SSN card or their number is fraudulently used, they can internally apply for a replacement SSN card or a new SNN number for their end.[31]

3.3.7 Enrolment

The UIDAI is the primary body that issues Aadhaar numbers. Registrars (contracted bodies under the UIDAI and enrolling agencies) are accountable for receiving and processing enrolments into the UID scheme. Social Security Agency (SSA) is the primary body in the US that receives and processes applications for SSN and issues SSN numbers.[32]

[29]Social Security History 1993 - 2000, Chapter 6: Program Integrity. Available at: www.ssa.gov.

[30]UIDAI, Lost EID/UID Process. Available at: uidai.gov.in

[31]SSA. New or Replacement Social Security Number Card. Available at: www.ssa.gov.

[32] Social Security. Availabl at: www.ssa.gov/

3.3.8 Details and Documents Required For Issuing Number:

Aadhaar application form requires following details and documents for the issuance of Aadhaar Number

a. Name
b. Date of birth (with proof like birth certificate or school leaving certificate)
c. Gender
d. Address (with proof showing that such person stays at given address like electricity bill, telephone bill, gas bill, etc)
e. Parent/guardian details.
f. Email
g. Mobile number
h. Consent or non-consent for sharing information provided to the UIDAI with Public services including welfare services. However, giving consent is the only option the public has.
i. Choice of the individual, permitting UIDAI to facilitate the opening of a bank account linked to the Aadhaar number and permits the sharing of information for this purpose. (this section provides option to the enroller but government has made it mandatory for banks to take Aadhaar as a proof to open an account at the bank)
j. If the individual has no particular objection to linking their present bank account to the Aadhaar number and all relevant bank details. (Out here too positive consent is the only option for the enroller as one cannot deny linking Aadhaar with bank)
k. Signature of the individual.
l. Thumb impression (impression is taken at the time of enrolment process)[33]

SSN application form requires following proof for issuance of the Number

a. Name to be shown on the citizenship card
b. Full name at birth, if different
c. Other names used
d. Mailing address
e. Citizenship or alien status

[33] Aadhaar enrollment/correction form. Available at: hstes.in, visited on 23rd September 2018.

f. Sex
g. Race/ethnic description (SSA does not receive this information under EAB)
h. Date of birth
i. Place of birth
j. Mother's name at birth
k. Mother's SSN (SSA collects this information for the Internal Revenue Service (IRS) on an original application for a child under age 18. SSA does not retain these data.)
l. Fathers' name
m. Father's SSN (SSA collects this information for IRS on an original application for a child under age 18. SSA does not retain these data).
n. Whether applicant ever filed for an SSN before
o. Prior SSNs assigned
p. Name on most recent Social Security card
q. Different date of birth if used on an earlier SSN application.
r. Date application completed
s. Phone number
t. Signature
u. Applicant's relationship to the number holder.[34]

It was stated in the news in 2014 that, UIDAI (Unique Identification Authority of India) had filed complaints against 3 firms for illegal use of Aadhaar biometrics.[35] Recently on a blog post[36] on Medium by user St_Hill shows that a simple Google search query returns excel sheets of 1000s of people's information including name, DOB, address, and Aadhaar number. This is a major concern as Section 29 of the Aadhaar Act states that:

"No Aadhaar number or core biometric information collected or created under this Act in respect of an Aadhaar number holder shall be published, displayed or posted publicly, except for the purposes as may be specified by regulations."

[34]Social Security Administration, Application for a Social Security. Available at: www.ssa.gov, visited on 23rd September 2018.

[35]www.timesofindia.indiatimes .com, visited on 25th October 2018.

[36] www.medium.com, visited on 17th October 2018.

No clear redressal is provided under the Act for an individual who is aware of the misuse of his Aadhaar number. In chapter 7 of the Aadhaar regulations, there is a clause for a grievance redressal mechanism whereby a person can potentially approach a call centre via phone or email which will inherently provide residents with a tracking number till the matter is closed. This is not enough, as the call centre is not equivalent to any public authority and hence its order cannot be considered authentic. There is no specification to give you a reason if they don't agree with you and why they can't help you. The process does not comprehensively ensure that people's dispute will be determined by the principles of natural justice.

All other countries including US and France are also tackling issues such as information leaks to terrorists and identity thefts. UK has removed the entire programme way back in 2010, after public objections that the programme was infringing upon civil rights. The Government of India is also required to implement safeguards and set up a full proof system for maximum benefit of the Aadhaar Cards with minimal risks.

4. CONCLUSION

Merging of multiple databases is an inescapable consequence of UID project. UID number would gradually become a common point which links all those databases to which the government has assigned contract for collecting and processing data under UID scheme. Over time, corporates could also adopt the UID Number as an identifier for the purposes of the efficient delivery of their services or even for enrolment as a customer. Eventually the separation of data that currently exists between different kinds of databases will vanish. A huge interlinked public information database has never been formed in India. It is also necessary that suitable actions are taken to protect personal data before the vast government store-houses of data are linked up and there is a real threat to data security and data gets misused.

The private sector companies such as banks, telecom companies, hospitals etc. are all collecting major amount of personal and non-personal information concerning individuals. This could lead to commercial exploitation of this information without the

consent/knowledge of the individual concerned and may lead to embarrassing an individual whose personal details can be made public by any of these private entities. The IT Act does give basic safeguards against disclosure of data/information stored electronically, but there is no comprehensive legislation for protecting the privacy of individuals for all information that may be in possession with private entities.

In the aforesaid circumstances information about an individual weather it is private or non-private is to be protected in view of the Government and private sector entities. Other than concerns around the risks faced due to this vast interconnected public information database, there are also some issues that are raised about the need for a separate legislation in the first place. The Aadhaar Card privacy issue become a matter of grave concern when the case reached Supreme Court.

Developing nations like India and China are finding it difficult to make their laws at par with the EU's stringent data protection policies. This adversely affects all trade between countries which don't have laws for data protection. The EU's Data Protection Directive allows personal data to be transferred to third countries (i.e. countries outside of the EEA) if that country gives an adequate level of protection. The US is not self-sufficient however the personal data sent under the Safe Harbor scheme is adequately protected. As of now India is not deemed to offer adequate protection. It has become an industry standard practice to use the EC model clauses when EU-based outsourcing involves data transfer and offshore processing in India. Such clauses alternatively allow data transfer, and place strict compliance obligations on both parties to ensure privacy of data and are considered by some to be tedious and to act as a disincentive for business

Most of India's IT and BPO industry comes from customers which are currently present in the European market. Industry representatives are concerned if India will be able to defend and grows the share of the European outsourcing market. As reported in the Economic Times of India, according to Ameet Nivsarkar, vice-president of Nasscom, the trade association represents the Indian software industry, "if European companies particularly insist on data secure status as a parameter for giving business, it will become a very important factor for perception of a country. Nonetheless, most of our companies adhere to very high level of data security." India has a splendid record of

performing at low end data processing but aspired to move up the value chain into more sophisticated and critical outsourced work in sectors such as healthcare, clinical research and engineering design.

The Data Security Council of India estimated that outsourcing business could rise by around $50 billion if India gets the status of a "data secure" destination. [37] India has demanded for getting to grant as a data secure status by the EU and incorporating a further investment protection clause in the Free Trade Agreement. However, India has not been granted data secure status by EU and therefore it has restricted the flow of data. Flow of sensitive information to India (such as information about patients for telemedicine) is obstructed according to the data protection law in EU. [38]

This also creates issues in the movement of people through restrictions on business development as it physically restricts any transfer of personal data to locations outside EU and allows it only if the importing country ascertain adequate data protection. Such circumstances raises day to day operating costs for Indian companies, thereby affecting competition and decreasing confidence of European firms in doing business in India. India has long been arguing that since US has a safe

harbour pact with the EU, and that the US and India have a data adequacy agreement; therefore, going by that rationale EU should give data adequacy status to India. The European Commission has been stating that issue of data protection adequacy should not be mixed with Free Trade Agreement and that India must meet the EU requirements for adequacy as per the process set in the 1995 Data Protection Directive. The Indian government thereby argues that the existing laws meets requisite EU standards and is fully compliant with the European data protection law.[39]

[37] Dr. Dinoj Kumar Upadhyay, India-EU FTA: Building New Synergies, Indian Council for World Affairs, November 2012, www.icwa.in.

[38] Deepak Rao, What to expect from the India-EU FTA, www.gatewayhouse.in

[39] India to EU: Declare us a data secure country, Times of India, October 2012, Available at: articles.timesofindia.indiatimes.com.

While comparing data protection laws of developed countries and Indian law, it gives a clear picture that the Indian laws need to at all times be evaluated and reviewed in order to maintain legal compliance. As per the Data Protection Directive, Organizations involved in storing personal data should register themselves with information commissioner, who gets appointed by the government as a representative of the government to keep a check on the rules and regulations provided by the Directive.

The Directive states that there are certain restrictions on the collection of personal data. Any personal data must usually be achieved only via lawful ways and should not be processed or used apart from the original purpose that it was desired for. The personal data should be appropriate, necessary in terms of quantity, accurate and overall sufficient for the purpose for which it is collected and processed. European Union and U.S try to protect the data and more specifically personal data of their citizens and they keep on trying to regularly upgrade their system according to the development in technologies.

US have a sectoral approach which comprises of varied legislation and regulations and self-regulations too. Data is categorised in number of types based on their usefulness in US. Therefore, different law arrangement is followed for each class of data. Indian IT Act deals with overall extraction of data, destroying of the data etc. which means that companies don't get any basic protection of data which mandates them to undergo separate contracts for making their data secured. The European Union mandates the protection of data on all its countries and the US too fulfils with the European Union in accordance with Safe Harbour Agreement and conducts normal business with the European Union countries. It has become very essential for India to adhere to the European Union for commercial reasons. Though efforts are made for Data Protection Act in India the legislature is unable to frame the Bill.

The IT act gives full protection to credit data which is a part of personal data aspects. So unauthorized use or transfer of data should be used to calculate and verify the credit worthiness of the customer and should be processed further later on. The IT Act, 2000 is quite generic Act which concentrates on relevant issues such as the digital signatures, cyber contraventions and offences, e-governance, confidentiality. The IT Act, 2000 is concerned with the issue of the Data Protection and privacy in a partial way

only. There is fundamentally a gap in actual framework in the IT Act, 2000 in matters of Data Protection Authority, quality and transparency of the data. Even if the IT Act, 2000 adopts some new changes still there is a lack of the actual framework for data protection and privacy for it to be on par with EU directive, OECD Guidelines or the Safe Harbour Principles.

Lack of Data Protection Law in India is major loss to the outsourcing industry since it is a flourishing industry in India. The customers of US and European Union are protected by the comprehensive law which requires that the personal data cannot be transferred at all to any countries which do not have adequate protection policy. The European trade Union stresses that data protection is a major issue which must be taken into account in these international out-sourcing companies. Hence India needs to handle this situation tactfully and should always the overall importance for the need of a Data Protection Act.

Cases relating to data theft from the call centres in India have played a major role urging the need for developing data protection law. Without a proper Data Protection Legislation, foreign customers are relying upon contractual obligations for safeguarding and storing of all data. Foreign customers are realising that such contractual obligations are not the best solution. In the event there is a breach of the data security, getting effective remedy redressal under the contracts obligations is itself tedious and time consuming. Having appropriate statutory protection with standard statutory penalties, damages and other remedies would act as a good deterrent for any corporate acting against the breach of data privacy.

In comparison to the European countries Indian cyber law system is also very poor and quick amendments to cyber laws are not possible, but it is very important to actually bring in the appropriate cyber law and awareness about cyber-crimes amongst the public. The outsourcing companies in India which deals with international personal data and information, it is mandatory requirement that there is an appropriate legal framework which gets introduced before it becomes too late and the progressive industry of outsourcing comes to a halt in India. On a rational point, it is a hurdle for India not to have any proper and adequate legal framework for personal Data Protection and Privacy of Data. The European Union official have published a list of countries

providing adequate data protection which includes Argentina, Canada, Australia and Switzerland, while India still needs to undertake many steps to get enrolled in this list. Passing the European Union standards can make India qualified to import data from many other data concerned countries.

Since the government delayed the implementation of a legal framework for prosecution of data and privacy breaches, Indian BPO companies have therefore implemented unified processes such as the BS7799 and the ISO17799 standards for information security management, which also explicitly restrict the quantity of data that is available to employees of BPO and call centres.

Indian government needs to implement a strong Data Protection Act to sustain the BPO business and parallely have a secured Aadhaar Card system. Still if the government still doesn't act on an effective data protection then a there are chances that India may completely loose BPO business and if data is misused under Aadhaar Scheme than it can lead to a undesirable result and can even cause threat to the nation once huge amount to citizen record is easily accessible without any proper protection.

CHAPTER 6

CONCLUSION AND SUGGESTIONS

Table Of Contents

1. INTRODUCTION

India started liberalizing its economy from 1990 and since then a huge upsurge in the IT business process outsourcing may be witnessed. Financial, educational, legal, marketing, healthcare, telecommunication, banking etc are only some of the services being outsourced into India. This upsurge of outsourcing of ITES into India in the recent past may be attributed to the large English-speaking unemployed populace, cheap labour, enterprising and hardworking nature of the people etc. Statistics have shown that the outsourcing industry is one of the biggest sources of employment. In a span of four years, the number of people working in call centers in the country supporting international industries has risen from 42,000 to 3,50,000.[1] Exports were worth $5.2 billion in 2004-2005 and are expected to grow over 40% this fiscal year. US is currently the biggest investor in Indian ITES, taking advantage of cheap labour costs. Statistics indicate that software engineers with two-year's experience in India are being paid about 1/5th of an equivalent US employee.[2]

With globalization and increasing BPO industry in India, protection of data warrants legislation. There are reasons for this. Every individual consumer of the BPO Industry would expect different levels of privacy from the employees who handle personal data. But there have been situations in the recent past where employees or systems have given away the personal information of customers to third parties without prior consent. So other countries providing BPO business to India expect the Indian government and BPO organizations to take measures for data protection. Countries with data protection law have guidelines that call for data protection law in the country with whom they are transacting. For instance, in, the European Union countries according to the latest guidelines, they will cease to part with data, which are considered the subject matter of protection to any third country unless such

[1]How secure are India's call centers- Soutik Biswas, available at news.bbc.co.uk.
[2] Data protection and offshoring to India, available at www.out-law.com, visited on 12th January 2016.

other country has a similar law on data protection. One of the essential features of any data protection law would be to prevent the flow of data to non-complying countries and such a provision when implemented may result in a loss of "Data Processing" business to some of the Indian companies.

2. VARIOUS CONCEPTS UNDER DATA

2.1 Concept Of Data

Data means collection, compilation or representation of information, knowledge, facts, concepts or instructions which are prepared or have been prepared in a formalized manner, and is intended to be processed or has been processed in the computer system or computer network, and may be in any form (including computer printout magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of computer. The term 'data ' is very wide in its area and scope. It covers both personal prospect of an individual and also commercial prospect. The individual prospects are protected as privacy rights while the commercial prospects are protected as proprietary rights. The expression data protects both privacy as well as proprietary rights.

2.2 Concept Of Personal Data

Personal data are defined as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;" Data are "personal data" when someone is able to link the information to a person, even if the person holding the data cannot make this link. Some examples of "personal data" are: address, credit card number, bank statements, criminal record, etc. The personal data also includes written or spoken communications as well as

images,[3] including closed-circuit television (CCTV) footage or sound.[4] Information recorded through electronic media, as well as information on paper may be personal data; in the modern time even cell samples of human tissue may be personal data, as they record the DNA of a person.

2.3 Concept Of Sensitive Personal Data

The definition of sensitive data, both Convention 108 (Article 6) and the Data Protection Directive name the following categories:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions, religious or other beliefs; and
- personal data concerning health or sexual life.[5]

3. URGE FOR THE DATA PROTECTION LEGISLATION

Information is the lifeblood of a knowledge-based economy. The control of data and the ability to translate them into meaningful information is indispensable to businesspeople, policymakers, scientists, engineers, researchers, students, and consumers. Having useful, and at times exclusive, information improves productivity, advances education and training, and helps create a more informed citizenry.

In the past two decades, those who collected or obtained access to a large amount of data began to explore ways to use the collected data as an income stream. In recent years there has been a growing fear about the large amount of information about individuals held on computer files. In particular it was felt that an individual could easily be harmed by the existence of computerized data

[3] ECtHR, Von Hannover v. Germany, No. 59320/00, 24 June 2004; ECtHR, Sciacca v. Italy, No. 50774/99, 11 January 2005.
[4] ECtHR, Peck v. the United Kingdom, No. 44647/98, 28 January 2003; ECtHR, Köpke v. Germany, No. 420/07, 5 October 2010.
[5] Article 8 of the Data Protection Directives.

about him/her which was inaccurate or misleading and which could be transferred to an unauthorized third party at high speed and very little cost.

Maintaining of data bases is not as much difficult task as maintaining its integrity, so in this era the most concerned debate is going on to innovate a perfect method of data protection. With the advancement in technological development, there took place a transition in the standard of crimes. In the present era most of the crimes are being done by the professionals through the easiest medium i.e. computers and electronic gadgets. Just by the single click, the criminals are able to get the secured information. The lust of information is acting as a catalyst in the growth of cyber-crimes. It is the very big headache for the business houses, financial institutions and the governmental bodies so as to give adequate protection to their huge data. In the absence of any stringent law relating to data protection, the miscreants are gaining expertise in their work day by day.

Though this world simplified our life style but it left certain anomalies in procurement of its object which resulted in involuntary disclosure of data. This can be analyzed from theses illustrations:

- On every login to the e-mail account in the cyber cafes, the electronic trail of password remained left there unsecured.
- On every use of credit card for purchasing purpose, the trail of brand preference, place of shopping etc. left behind.
- On every login to internet, there left behind an electronic trail enabling website owners and advertising companies to get access to the preference and choices of the users by tracking them.
- Employees are under seizing, as employers routinely use software to access employee's e-mail and their move.
- Phone call signals of the police are easily tracked by the naxalites enabling them to know about the police plans.
- Source code theft is the most preferred act of the miscreants.

- Unsolicited e-mails are also a usual practice of gathering personal information of the users.
- Movement across the web can be tracked by placing cookies and then retrieving such a way that allows building detailed profile of the user's interest, spending habits and lifestyle.
- Through hacking, the hackers can whimsically alter anyone's account.

Thus it can be easily pointed out that how easy we are providing room to the miscreants to enhance and simplify their acts and how safe is it to avail the services of the digital world.

Data protection focuses on issues relating to the collection, storage, accuracy and use of data provided by Net users in the use of the World Wide Web. The type of information collected by operating websites can be classified as either individually identifiable information or Mass undisclosed information:

- Individually identifiable information can be defined as information that can be used to identify an individual, that consist of information like name, address, telephone number, credit card number, or email address and other consumer specific information. Also IP address is associated with Personally Identifiable Information. The Internet generates an elaborate trail of data every stop a person makes.
- On the other hand, Mass undisclosed information" can be defined as information that: a website or third party on its behalf aggregates and categorizes by established geographical areas, such as postal codes and contains non-consumer specific information created from anonymous transactions for use by merchants in better managing their businesses and conducting mass media advertising.

There is abundant of technologies that are utilized to collect both Classes of information on consumers. Such a piece of information [computer code] is saved on your own Computer or your browser. It contains information as to the

personal preferences exhibited when visiting a website. As it is impossible to differentiate between Visitors to a Web site, the server will somehow mark the visitor by storing information on them.

The situation now warrants protection for data. Visitors to any website want their privacy rights to be respected when they engage in e-Commerce. It is part of the confidence creating role that successful e-Commerce businesses have to convey to the consumer. If industry doesn't make sure it's guarding the privacy of the data it collects, it will be the responsibility of the government and it's their obligation to enact legislation.

The problem that arises in e-Commerce is that the Internet is in itself global. Generally the regulations of the Government will have very little impact unless they are part of a larger international setting. The protection of personal data has never been a purely national problem; it was always a global issue.

Previously, data were protected primarily for their ability to enhance the value of other goods or services, rather than for their inherent value. Secrecy, family control, or the use of physical devices, like locks and safes, often protected valuable data, such as those contained in customer lists, inventory files, and sales records. As the legal system became more developed and as sophisticated technologies emerged, trade secret, misappropriation and unfair competition laws, contracts, and technological protection measures are being gradually deployed to offer additional protection.

With the beginning of national programmes like Unique Identification number, NATGRID, CCTNS, DNA profiling, Reproductive Rights of Women, Privileged communications and brain mapping, most of which will be implemented through ICT platforms, and bigger collection of citizen's information by the government, apprehensions have raised on their effect on the personal information of the citizen. Information according to the routine

has begun to be collected on a regular basis through statutory requirements and through e-governance projects. This personal information includes data related to: health, travel, taxes, religion, education, financial status, employment, disability, living situation, welfare status, citizenship status, marriage status, crime record etc. At the moment there is no principle policy speaking to the collection of information by the government. This has led to doubts upon who is allowed to collect data, what data can be collected, what are the rights of the individual, and how the information so collected will be protected. The volume of personal information being held by various service providers, and the potential for data convergence that digitization carries with it, is a matter that raises issues about data protection.

Global data flows, today, are now not same as a file transfer that an individual's action initiated for point-to-point transfer over 30 years ago. As soon as a transaction is initiated on the internet, multiple data flow takes place simultaneously, via phenomena such as web 2.0, online social networking, search engine, and cloud computing. This has led to ubiquity of data transfers over the Internet, and enhanced economic importance of data processing, with direct involvement of individuals in trans-border data flows. While this is exposing individuals to more privacy risks, it is also challenging business which are collecting the data directly entered by users, or through their actions without their knowledge, e.g. web surfing, e-banking or e-commerce and co-relating the same through more advanced analytic tools to generate economic value out of data. The latter are accountable for data collection and its use, since data has become one of the drivers of the knowledge based society which is becoming even more critical to business than capital and labour.

The private sector on the other hand, uses personal data to create new demands and build relationships for generating revenue from their services. The individuals are putting out their data on the web in return for useful services at almost no cost. But in this changed paradigm, private sector and the civil society have to build legal regimes and practices which are transparent and which inspire trust among individuals, and enhance their ability to control

access to their data, even as economic value is generated out of such data collection and processing for all players.[6]

The urge to protect data along with privacy protection in India is relatively new, coming out from the constantly growing off-shoring business carried out in India by foreign companies where data is exported by these foreign companies to their off-shore agents or counterparts in India.[7]

3.1 EU Regulation of January 2012:

Several new principles and changes to existing principles were suggested by the EU Regulation of January 2012 for the protection of data. These include:

- More explicit expression of the "data minimization" principle and will require companies to limit the amount of data they collect much more strictly.[8]
- Accountability of data controllers by requiring that personal data be processed under the responsibility and liability of the controller. The data controller is also responsible for compliance with the Regulation.[9]
- Right to object by the data subject for the sending of direct marketing; Opt-in consent is, however, not required.[10]
- Data controllers bear the burden of proof in showing that data subjects consented to the subject of personal data.[11]
- Expands the definition of sensitive data to also include genetic data and data concerning "criminal convictions of related security measures".[12]

[6] Report of the Group of Experts on Privacy

[7] Jürgen Schaaf and Thomas Meyer, Outsourcing to India: Crouching Tiger Set to Pounce (Deutsche Bank Research), Oct. 25, 2005, available at www.dbresearch.com, visited on 29th April 2015.

[8] Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data on the free movement of such data (General Data Protection Regulation) Available at: ec.europa.eu

[9] Article 8 to 22 of EU Regulations

[10] Article 19(2) of EU Regulations

[11] Article 7(1) of EU Regulations

- Right to be forgotten and to erasure: Data must not be retained indefinitely and time limits must be set in place after which data must be erased from the system.[13]
- Data controllers must have "transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights"
- Right to data portability allowing individuals to change online service providers.[14]
- Regulate the use of "Profiling"[15]
- Accountability of data controllers, and independent verification of compliance measures.[16]
- Data controllers implement "appropriate technical and organisational measures" including Privacy by Design, and Privacy by default.[17]
- Data controllers subjected to wide-ranging data security obligations.[18]
- Data breach notification requirement applicable to all types of data controllers, notification of a data breach to be given by a data controller to both its Lead DPA and to the data subjects concerned.[19]
- Data protection impact assessments are to be carried out by data controllers and data processors.[20]
- Data protection officers mandatory for all public authorities and for all companies with more than 250 employees.[21]
- The Regulation also foresees drafting of codes of conduct covering various data protection sectors, and allows them to be submitted to DPAs, which may give an opinion as to whether they are "in compliance with the

[12]Article 9(1) of EU Regulations

[13] Article 17 of EU Regulations

[14] Article 18 of EU Regulations
[15] Article 20 of EU Regulations
[16] Article 22 of EU Regulations
[17] Article 30(3) of EU Regulations
[18] Article 30 of EU Regulations
[19] Article 31 of EU Regulations
[20] Article 33 of EU Regulations
[21] Article 35(1)(b) of EU Regulations

Regulation".[22] Compliance with a code of conduct may be deemed to satisfy the legal requirements of the proposed Regulation. Article 39 establishing "data protection certification mechanisms and of data protection seals and marks", is encouraged, though the legal effect of such recognition needs to be clarified.[23]

3.2 US Consumer Privacy Bill of Rights

The US Consumer Privacy Bill of Rights states that consumers have a right to:

- Consent, Notice/Choice: Individual Control over what personal data companies collect and how they use it.
- Transparency: Transparency through easily understandable and accessible information about privacy and security practices.
- Limitation: Respect for Context: that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
- Safety/Security: Secure and responsible handling of personal data.
- Access, Alterations and Accuracy: access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.
- Focused Collection: reasonable limits on the personal data that companies collect and retain.
- Accountability: personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.[24]

3.3 OECD Privacy Principles

The discussion on revision of OECD privacy principles has revolved around three topics:

[22] Article 38(2) of EU Regulations
[23] Article 39` of EU Regulations
[24] Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. Available at: www.whitehouse.gov.

(1) The roles and responsibilities of key actors;

(2) Geographic restrictions on data flows; and

(3) Proactive implementation and enforcement.

The revised OECD Guidelines emphasises on efforts to educate and raise awareness of privacy risks and ways to mitigate them. By emphasizing transparency and individual consent, the current privacy framework imposes significant, sometimes unrealistic obligations on both businesses and individuals. On the one hand, businesses are expected to explain their data processing activities on increasingly small screens and seek consent from often-uninterested individuals; on the other hand, individuals are expected to understand complicated privacy disclosures and knowingly consent to them. It is not clear as to the role that consent should play in an age where data flows become increasingly complex, multiple parties are involved, and information is provided to individuals with short attention spans on increasingly small screens? What is the right balance between individual consent on the one hand and efficiency or legitimate business interests on the other hand.

The OECD Privacy Guidelines have long recognized that consent is not the *sine qua non* of data processing. The "collection limitation principle", for example, states that "data should be obtained by lawful and fair means and, *where appropriate*, with the knowledge or consent of the data subject".

Proactive implementation and enforcement elaborate the accountability principle to feature concepts like privacy by design and data breach notification. Undertake analysis of the economics of remedies and sanctions by enforcement authorities, as well as trying to enhance international regulatory cooperation and interoperability of regulatory frameworks.[25]

[25] OECD Privacy Principle. Available at: oecdprivacy.org/

4. CONFLICTS BETWEEN DATA PROTECTION LEGISLATION AND OTHER LAWS OR IDEOLOGIES

There have been various concerns voiced about the fact that the enactment of a data protection regime will conflict with some already existing and necessary legislations. Can a data protection law co-exist with these statutes?

4.1 Data Protection And The Right To Information

There are questions raised about whether the rights granted by data protection legislation would run contrary to the rights available under the Right to Information Act which provides citizens the right to access public information. Answer to this can be that, data protection legislations exist around the world even in countries that have enacted detailed public information access legislations. These two types of laws have been proven to be capable of existing together. Rather being contrary, they operate antipodal from each other and give each other meaning.

The right to information under the RTI Act relates to such information as is available with a public officials including work, documents, records, sample of information etc. which a citizen has a right to access. This, in itself, is the inbuilt protection available for data including personal information. Thus, just as an individual has the right to access public information, he has the right to prevent unauthorized access to his personal information which is a part of data protection. In fact, there are several provisions in the RTI Act itself which directly or indirectly reinforce that private information relating to an individual is to be prevented from unauthorized disclosure. For example, Section 11 prescribes that information relating to or supplied by a third party which has been treated as confidential by the third party cannot be disclosed without his / her consent. As such, a well-defined separate data protection regime will be co-acting to the provisions of the RTI Act.

However, despite the existence of a specific exemption under Section 8 of the RTI Act, there is still no clarity as to whether the personal data of public officials falls within the exemption. Under the RTI Act, it might be possible for citizens to claim a public interest in accessing personal information of such public servants and given that the law does not make this clear, could use this provision to invade the personal privacy of a government servant. Hence, it must be made clear under the RTI Act that the personal information of the government servant can be made accessible to the public in order to avoid any conflict with the data protection regime.[26]

4.2 Data Protection And Credit Verification

Credit verification is the core upon which modern banking systems are based. In that context, banks and financial institutions rely upon the ability to access personal information about prospective borrowers in order to be able to assess whether or not they should be granted a loan.

Data protection statutes do not restrict collection of data. They just control the manner in which data is collected and processed. Most data protection legislations limit the processing of the personal information for the purpose for which it was collected. Accordingly, so long as personal information provided for verifying the credit-worthiness of a person is used for that purpose alone, there would be no problem using such information under the proposed data protection legislation at the end of the thesis. Moreover, the option of consent is also available to the data subject. If a data subject needs loan or other things he need to give consent for the access of his personal information for the purpose of verification.[27]

[26] Approach paper for a legislation on privacy, published by Government of India, Ministry of Personnel, PG & Pensions Department of Personnel Training on 25th October 2010.
[27] Approach paper for a legislation on privacy, published by Government of India, Ministry of Personnel, PG & Pensions Department of Personnel Training on 25th October 2010.

4.3 Data Protection And Private Investigative Agencies

There is a further potential conflict between the business of private surveillance and investigation and data protection. Would the enactment of a data protection law result in the curbing of the freedom to trade of detective agencies?

A number of European countries have specific enactments dealing with the use of scrutiny for security and private investigation purpose and the review of information obtained. Private investigators have to be licensed in many countries. In Ireland, it is necessary that physical and electronic surveillance measures must comply with data protection laws. Given that private detective agencies, if allowed to operate without regulation, could potentially inflict considerable mess on the personal information of a citizen, it is important to ensure that these agencies are regulated particularly when it comes to the use of personal information. The introduction of data protection legislation could have significant consequences on this industry.[28]

4.4 Data Protection And National Security

There is likely conflict between data protection needs of an individual and interests of national security. On many occasions Government may need to resort to gaining access to personal information and it's sharing with other government agencies in order to safeguard national interests. [29] Hence, in the below proposed data protection legislation national security has been placed as one of the main reason for exemption from the law.

4.5 Data Protection Vs. Transparency In Government

In recent times, the government has, in order to demonstrate greater transparency in its functioning and reduce corruption, initiated the practice of publishing complete details of all the government activities with full

[28] Approach paper for a legislation on privacy, published by Government of India, Ministry of Personnel, PG & Pensions Department of Personnel Training on 25th October 2010.
[29] Approach paper for a legislation on privacy, published by Government of India, Ministry of Personnel, PG & Pensions Department of Personnel Training on 25th October 2010.

information about the recipients of government service. While these initiatives do go a long way to validate the fact that government servants have honestly and without fraud or corruption, delivered the services they are obliged to provide, they have the unintended consequence of exposing vast quantities of personal data in a very public way.

With the introduction of the UID number this practice could result in even greater harm as the UID number that will be present in each and every publication of this nature will make it easy to link various public databases and help create an identifiable profile of everyone on that public database. The government needs to balance the need for transparency with the social obligation to provide its citizens with personal privacy and data protection. A stringent separate legislation for data protection would complement the Aadhaar Act enacted by the government for the protection of the details collected by various agencies in order to provide Aadhaar number to the citizens of India.[30]

5. ***CONCLUSION***

Data protection has emerged as an important reaction to the development of information technology. In India data protection is covered under the Information Technology Act, 2000 (hereinafter, the Act). The Act defines 'data' as, "'data' means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer".[31] Protection of such data and privacy are covered under specific provisions in the Act.[32] In the recent past, the need for data protection laws has

[30] Approach paper for a legislation on privacy, published by Government of India, Ministry of Personnel, PG & Pensions Department of Personnel Training on 25th October 2010.
[31] The Information Technology Act, 2000, Sec. 2(1)(o)
[32] The Information Technology Act, 2000, Sec. 43, Sec. 65, Sec. 66, Sec. 72

been felt to cater to various needs. The following analyses the position of data protection law with respect to some of the needs.

In the recent past, concerns have been raised both within the country as well as by customers abroad regarding the adequacy of data protection and privacy laws in the country.[33] A few incidents have questioned the Indian data protection and privacy standards and have left the outsourcing industry embarrassed. In June 2005, 'The Sun' newspaper claimed that one of its journalists bought personal details including passwords, addresses and passport data from a Delhi IT worker for £4.25 each.[34] Earlier BPO frauds in India include New York-based Citibank accounts being looted from a BPO in Pune and a call-center employee in Bangalore peddling credit card information to fraudsters who stole US$398,000 from British bank accounts. UK's Channel 4 TV station ran broadcast footage of a sting operation exposing middlemen hawking the financial data of 200,000 UK citizens. The documentary has prompted Britain's Information Commissioner's Office to examine the security of personal financial data at Indian call centers.[35]

In April 2017, news are heard for call centre fraud in Ahmedabad as well as Mumbai and a person named Sagar Thakker alias Shaggy Thakker has been arrested for the same from Dubai. Shaggy Thakker was running call centres at Ahmedabad and Mumbai where data of USA use to flow for the process. Shaggy Thakker misused the data collected at the call centre and use to call person at USA for paying their dues under the disguise of the agent of bank. In this way her extorted lots of money from the resident of USA, thus making fraud and not fulfilling the conditions laid in the contract he made. Hence, this shows that the existing laws applicable in India needs to revive and must be made stringent. Many call centers are being shut down by police for the fraud done into it. Thus, a codified stringent law can reduce such scams and can help to bring back the trust of countries transferring data from their country to India.

[33]India tightens Data Protection law available at www.atimes.com.
[34]How secure are India's call centers- Soutik Biswas, available at news.bbc.co.uk.
[35]India tightens Data Protection law available at www.atimes.com.

With globalization and increasing BPO industry in India, protection of data warrants legislation. There are reasons for this. Every individual consumer of the BPO Industry would expect different levels of privacy from the employees who handle personal data. But there have been situations in the recent past where employees or systems have given away the personal information of customers to third parties without prior consent. So other countries providing BPO business to India expect the Indian government and BPO organizations to take measures for data protection. Countries with data protection law have guidelines that call for data protection law in the country with whom they are transacting. For instance, in, the European Union countries according to the latest guidelines, they will cease to part with data, which are considered the subject matter of protection to any third country unless such other country has a similar law on data protection. One of the essential features of any data protection law would be to prevent the flow of data to non-complying countries and such a provision when implemented may result in a loss of "Data Processing" business to some of the Indian companies.

There has been a strong opinion that if India strengthens its data protection law, it can attract multi-national corporations to India. India can be home to such corporations than a mere supplier of services. Apart from this a large data has been collected by the private agencies for Aadhaar card; this Aadhaar number contains personal details of the citizen of India. Hence, protecting Aadhaar number under a stringent law is much more necessary to avoid any disastrous offence which can bring an innocent citizen under severe trouble.

Once the data protection law is enforced in India, companies outsourcing to India are unlikely to dismantle the systems they have in place straightaway, and move data more freely to India. Hence, the need for data protection laws would win over the confidence of international business partners; protect abuse of information; protection of privacy and personal rights of individuals would be ensured; there would be more FDI inflows, global

business and the establishment of research and development parks in the pharmaceutical industry & impetus to the sector of e-Commerce at national and international levels would be provided.

If it was not for this rapidly increasing off-shoring business and the Unique Identification Number programme, India would perhaps never have worried much about data protection, as there are already existing provisions in the Indian legal framework for protection of data, though not at the scale at which protection is warranted under the current circumstances. The Aadhaar number, which is a single global identifier that is supposed to work across application domains, makes individuals vulnerable to privacy breaches. In an Aadhaar like setup, the biggest threat to privacy comes from potential insider leaks. The Aadhaar programme does not seem to have been explicitly designed to have strong protections against such insider leaks. We believe that effective protection against insider leaks necessarily requires a data controller at UID headquarters as well as at the companies hired for the collection of data on behalf of the government. UID programme has started and various complaints also have been registered against the company hired for collection of data by the government at several places. Thus, though there are serious privacy concerns at present, we believe that Aadhaar can be made safe from the legal perspective by enacting a legal framework for data protection for more specific significant strengthening. Perhaps the single most important specific question that begs answering is who should have the right to verify the identity of an individual, and under what circumstances? Though Aadhaar Act has been enacted but a stringent single codified law is needed for the better protection of data in India.

5.1 Proposed Framework For Data Protection Legislation

The framework for the data protection legislation should highlight the basic principles that any data controlling authority will need to subscribe to and how the data as well as privacy rights of an individual would be protected. The specified features of the framework are discussed below in detail:

5.1.1 Principles On Which The Proposed Legislation Is Based

The data protection principles are as follows:

1. Data shall be processed fairly and lawfully.
2. Data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Data shall be accurate and, where necessary, kept up to date.
5. Data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Collection, Process, Handling and Storage of Sensitive Personal Data must be done with extra care.
9. Personal data shall not be transferred to a country or territory outside India unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

5.1.2 Applicability

Almost all data protection legislations have a well-defined applicability clause, determining the persons who have to comply with the obligations set out therein. 92% of the countries have made their enactments applicable to both public and private entities. Most legislations exclude from the ambit of the legislation, information that is solely in the domestic or household sphere and for strictly personal reasons.

With the increasing digitization of data, many entities both public as well as private, have collected and currently hold vast amounts of personal as well as non-personal data of citizen of India. It is possible that public entities and governmental agencies currently hold much more data about a larger section of society than any private entity. There is currently no legislation that protects against the misuse of this data. Hence, the proposed data protection legislation at the end of this thesis applies equally to private as well as public entities.

5.1.3 Data

The legislations that were examined have made a distinction between personal data and sensitive personal data, applying a greater standard of care when dealing with sensitive personal data as opposed to personal data. Indian as a developing country in this context, it is advisable that such a distinction be brought about in order to ensure that all forms of identifiable data are protected under the general right to privacy but that a greater responsibility is imposed on entities processing or collecting certain categories of information which if disclosed could result in significant financial, reputational or other associated loss to the person concerned.

5.1.4 Personal Data

Almost all the legislations define personal data as a means which can make any person an "*identifiable person*". Unless the sum total of the information in question has the ability to identify a real person it will not be elevated to the status of personal data. In most cases, personal data refers to identity information about *natural* persons.

Some countries have come up with an appropriate definition for personal data that results in information that is capable of identifying a person, either directly or indirectly (and thereby causing risk to his identity), being included within the ambit of the definition. It is possible that a person could be identified directly by name or indirectly by his car registration number or passport number. It is important to include both types of data within the

definition. Equally, it is important to recognize that in all cases person's name may not be enough to identify him.

It is also important to bring all personal information within this definition regardless of the format in which the information is stored. For instance, video surveillance footage that identifies a person should be classified as personal data in order to protect the privacy of the person involved. For example, drawings made by patients as part of psychiatric evaluations should similarly be treated as personal information as they could identify the medical condition of the person.

5.1.5 Sensitive Personal Data

Definition of personal data is very wide while compared to sensitive personal data, which is more specific and includes various types of information, which, if disclosed inappropriately, could result in financial and reputational loss to the person concerned. Sensitive Personal Data includes within its ambit the following information:

- racial or ethnic origin;
- political affiliations or opinions;
- religious affiliations and beliefs or other beliefs of a similar nature;
- membership of a trade union;
- physical or mental health or condition;
- sexual life; and
- criminal record.

In addition, the following categories of information have also been treated as sensitive personal information in some legislation.

- Genetic information about an individual that is not otherwise health information;
- Information or an opinion about an individual;
- Financial or proprietary confidential corporate data;

- Data on a person's personality;
- Private family relations;
- Biometric data;
- Social welfare needs of a person or the benefits, support or other social welfare assistance received by the person; and
- Data collected on a person during the process of taxation (except data concerning tax arrears).

It is important that an appropriate list of items that would constitute sensitive personal information in the Indian context be developed. While the first list set out above must form the basis for any list of sensitive information that is to form part of the Indian legislation. Also, in the context of the Aadhaar program, it will be relevant to include biometric data in the definition of sensitive personal data. Financial and credit information should also be treated as sensitive personal data as it is a crucial information of an individual.

5.1.6 Data Collection

Many countries have data protection legislations which includes provisions that deal with and regulate the collection of data. These provisions usually include the following elements:

- It is necessary to inform the data subject of the purpose of the collection of data.
- The explicit or written consent of the data subject must be obtained for the collection of data.

However, the balance of interests must always be considered and in certain cases, the requirement to obtain consent may be dispensed with for reasons such as national security, benefit of the data subject or investigation of a crime or other circumstances that may be prescribed in the statute

- The data subject is free to withdraw consent in certain cases.

- The data that is collected must only be for specific, explicitly defined and legitimate purposes. For instance, the collection must be authorised under a law. The data subject must consent (such consent being subject to the test of "balance of interests") to his personal data being used for the specified purposes.
- Collection of data which is of a sensitive nature is generally subject to more control or may be prohibited. Explicit consent or even approval from a regulatory authority may be required to be obtained to collect sensitive personal data.
- Data collected must be proportional to the purpose for which it was collected.
- The information that is collected must be accurate and up to date.
- Where the information is not received directly from the data subject, the source of the information must be informed to data controller.

Looking at the Indian context, informed written consent should be where it is supported by the balance of interests. The need for written consent in local language or a language known to the subject must be examined. It will also be important to address concerns of illiteracy and the need to ensure that all persons who provide personal data understand why they are doing so and what the data is going to be used for. Informed consent is particularly important where information is being sought from people who do not have the ability to read and write and therefore to understand why the information is being sought. However it is important to recognize that in certain circumstances, such as in relation to the use by employers of personal information of their employees, customers, suppliers and shareholders in the conduct of their business, consent may not be necessary in all instances. Additional exceptions such as collection of data for investigation of criminal offence, national security, health, census etc. may be built in. An exception may need to be made in case of data which government agency collects and an individual is statutorily require to provide such as data for Census.

Data subjects should also be allowed to withdraw consent for data collection even after the data has been collected. The right to withdraw consent is integral to any right to personal privacy. The ability to collect data must come with an obligation to ensure that whenever a data subject wants to be removed from the database, such data subject should have the right to leave.

Data should be collected only for a specific stated purpose. Data once collected must only be used for the purpose for which it was collected. If a data controller is allowed to indiscriminately use the data collected, it would vitiate the informed consent obtained prior to collection. If the data is to be re-used for a different purpose the data subject should have a justiciable right against the data controller for allowing the data so collected to be used otherwise than for the purpose for which it was intended. Implicit in this provision is the obligation on the data controller to only collect that amount of data as is necessary for the stated purpose and no more.

The proposed data protection legislation will impose restrictions on the collection and use of data; it is in the interests of the general public that this restriction is imposed. Sensitive personal data must be treated differently from regular personal data. At present no Indian legislation makes this distinction and it is imperative that the country's data protection legislation creates these categories to ensure that some forms of personal data are treated more specially than others.

5.1.7 Data Processing

The legislations reviewed here include regulations with regard to data processing. Since most data leakage takes place during remote processing, is important to ensure that adequate measures are in place to ensure that data transferred to a processor receives the same level of protection. Most data protections legislations include the following provisions with regard to data processing:

- The data controller has to ensure that the data processor processes the information/personal data for the purpose for which it was collected.
- Data processing must be done carefully and in a diligent manner.
- Data processing must for reasonable and legitimate purposes and must be in good faith and in consideration of the interests of the individual.
- Data subject must have the knowledge of the purpose for which the data is being processed.
- Processing in a manner that provides unauthorised access of the data to persons other than the data subject is strictly prohibited.

Since the data controller has obtained consent from the data subject for the collection of data it should be the responsibility of the data controller to ensure that any processing that takes place by a third party processor is done with the same standards of data protection required of the data controller. The data controller must be responsible for the faults of the data processor and should be primarily responsible for compliance by the data processor with data protection obligations.

It is important that, in the event the data collected needs to be processed, the data subject is informed that it is going to be processed as well as why. Under various circumstances, digital data is processed automatically using computer algorithms. Many data protection legislations include specific provisions that allow data subjects to question such automated decisions. However, considering the population of India, the practical nuances involved in prohibiting the automated process must be considered. It is important that the individuals be informed of the reasons for which the data will be processed. The data processing must be proportional to the purpose for which it was collected and must be conducted in a diligent manner to avoid any disclosure or unauthorised access.

5.1.8 Data Storage

Data once collected needs to be stored and as larger volumes of data enter into public and private databases, the need to legislate on appropriate storage regulations becomes important. No matter how carefully regulated collection and processing might be, if data retention and storage regulations do not match up, there is a grave risk that this will prove to be the source of data violations. The legislations analysed here have regulations relating to the retention and storage of data. These include provisions such as:

- The data once collected must be deleted after achieving the purpose for which it was collected.
- Data must not be stored in a form that allows data subject to be identified after achieving the purpose of collection.
- Uniform personal identification numbers must not be used for identification of data subjects.
- Some of the exceptions for deletion of data include keeping data for historical, scientific and statistical or research purposes.
- The details of data collected to be published in register or in a website.
- Access to the data must be blocked if the data cannot be deleted.
- The data controller must limit the time period of the retention of information to the minimum necessary.
- The details of the time and date when the information is collected for storage must be noted.
- Data subjects must be provided with a mechanism to withdraw the consent at any time, without undue delay, cost or gain to the data controller.

It is important to ensure that the data is stored only till the time the purpose for which it was collected is achieved, unless the purpose is for archival purposes, national security purposes etc. Once the purpose has been achieved, the legislation should prescribe that the data so collected should be deleted permanently. It is also important to prevent the linking of databases. There are many merits to such linkages, particularly in the current social and economic circumstances of India. However, the possibility of misuse exists and

the consequences of misuse could far exceed the good that this might bring. If linkage is to be permitted adequate safeguards must be taken to ensure that such linkage does not result in invasion of personal privacy. Obligations to anonymise data or to otherwise protect data subjects from unlawful abuse of their information across databases should be included.

5.1.9 Data Security

The data once collected, will need to be stored, by the data controller. It is important that the proposed data protection legislation should impose adequate data security obligations on the data controller for the duration of such storage. Most data protection legislations have provisions such as:

- The data controller must ensure that the data is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse.
- The integrity of personal information to be secured by taking appropriate technical and organisational measures.
- Steps should be taken to prevent unauthorised access to personal data, including the right of physical access to the premises, data, and programs and to operate equipment of the data controller or processor.
- The identity of persons who have access to information network should be logged.
- The organisation must appoint specific staff (such as a security officer) to maintain security of data and prevent the data from burglary, alteration, destruction, extinction, or disclosure.
- Some laws also mandate technical procedures and measures to protect data while in transmission. This includes an obligation to transfer data only in cryptographic form with a digital signature.
- In some countries, the data regulator is responsible for ensuring credibility and integrity of the data controllers handling the information and for ensuring that equipment used is of a high standard.

- Some countries also vest an obligation on organisations to inform data subjects of security incidents that may lead to a threat of unauthorised disclosure of personal data.
- Privacy impact assessments to be conducted by independent authorities in the form of transparent audits, for the protection of personal data.
- Adoption of a code of practice to measure the efficiency and level of protection of personal data.
- A response plan to be formulated by organisations which will set out the appropriate action to be taken for breach of data protection laws.
- The technical and organisational measures to be undertaken by data controllers must be proportionate to the existing risk, sensitive nature of information and its consequence for the data subject.
- When processing is carried out by service providers, the controlling authority must enter into a contract that provides the scope, content, obligations and guarantee of compliance of data protection principles by these service providers.
- At the time of encountering a security breach during processing, the data subjects must be informed about the potential pecuniary and non-pecuniary effects of such a breach. This information must be provided well in advance.
- Mechanisms that prevent and detect breaches depending upon the standardised model of information security governance/management must be implemented.
- Periodic internal training, education and awareness programmes aimed at better understanding of data protection principles and security issues must be implemented.
- Data privacy officers with adequate qualification, resources and power for supervisory functions must be appointed to overlook functioning of data controllers.
- Response plan that establishes guidelines for verifying a breach of applicable law, cause and extent of breach, harmful effects and appropriate measures to avoid future breaches must be implemented.

- Data supervising authorities must ensure the following security standards are maintained:

(a) Supervisors must be impartial, independent and have technical competence and adequate resources to carry out their functions;

(b) Supervisors must ensure coordination to achieve uniform standards of data protection is maintained at national level, by sharing reports, investigative techniques and other necessary information; and

(c) Supervisors must maintain high level of confidentiality of information exchanged during course of co-ordination.

To the extent possible the legislation must prescribe the measures to be taken by the data controllers to ensure the security of data under its control. Care should be taken to ensure that the measures prescribed should be technology neutral as it is likely that data security measures will only improve in the future. The emphasis should be on ensuring that appropriate measures are taken with a view to achieving a prescribed and stated result. There should be no attempt at prescribing the means to achieving that end. It is recommended that the data must be protected again unauthorised access, deletion, disclosure and alteration. The onus to protect the data must be on the data controller. It may also be worth considering circumstances under which the data regulator could supervise the implementation of these measures.

5.1.10 Data Access

Once data has been collected it remains under the control of the data controller. If the data changes (such as in the event the data subject moves to a different address) it is important that this data be rectified and made current. Similarly, if the data subject finds, after his data has been collected, that the database entries are incorrect, it should be open to the data subject to rectify the database in order to rectify his own data. The data protection legislations studied here includes provisions such as:

- Data subject must have access to the data, subject to applicable laws. The subjects are also granted the right to rectify.

- In some countries, the correction of personal information can be made following an investigation.
- Some countries require that the data holder must produce relevant identity proof while requesting access to personal data.
- It is mandatory for the data controller to provide an individual with information with respect to data controller, the purpose of data collected and who are the recipients of the data, information on processing of the data etc.
- Information must be provided to the data subject by using clear and plain language. Special care must be taken with respect to information of minors.

In order to ensure that the database is accurate and up to date, specific provisions should be included to allow data subjects to rectify their own personal information. In fact, data subjects should always be allowed to review their information collected and stored in the database.

It is important to consider whether legal heirs, guardians and authorised representatives of the data subject should be granted access to personal information of their guardians or wards. This would also be relevant to consider in the context of deceased data subjects – for instance, would it be possible to conclude, after the death of a person, that he ceases to be a natural person and therefore is no longer protected under the statute? In all these circumstances adequate verification procedures must be implemented to ensure that personal information does not fall into the hands of persons not authorised to collect it.

5.1.11 Cross Border Applicability And Transfer

European countries extend the applicability of their data protection legislations to persons who may not be located within the country but may be using equipment located in the country, to process information. Most European legislations also prohibit the transfer of data to countries with less rigorous data protection laws. Our review indicates that 66% of countries analyzed, have

provisions that permit the regulator to prosecute non-residents in respect to data offences as long as the data in question is stored within the country and the storage was not merely for the purpose of transit.[36]

A strong data protection law will afford the opportunity for free flow of personal data from the European Economic Area to India. This would particularly benefit providers of outsourcing services located in India. However, it may be advisable to ensure appropriate measures to protect the data of Indian citizens that are processed outside the country. The legislation could include provisions that allow the regulator to proceed against data controllers not just for data protection violations committed within the country but also outside the country if the data concerned relates to an Indian citizen, or was collected by the data controller in India.

5.1.12 Exemptions

All data protection legislations have in-built exceptions that limit the applicability of the legislation in the context of certain statutorily established circumstances. These could include national security and interests, statutory functions, disclosures required by law or as part of legal proceedings, etc.

When analysed various data protection enactments around the world, the most common exemptions are on grounds of national security. Most countries also provide exemptions for the purpose of apprehension and prevention of offenders, protecting the public from financial loss, protecting charities against mismanagement, disclosures required by law or under legal proceedings, securing the health, safety and welfare of people at work, statistical or historical research purposes, assessment of collection of tax, processing for the publication of journalistic, literary or artistic material and discharge of a statutory function from the principles of data protection.

[36] Approach paper for a legislation on privacy, published by Government of India, Ministry of Personnel, PG & Pensions Department of Personnel Training on 25th October 2010.

There could be several specific exemptions that are particular to the Indian social and economic environment. In the Indian context, it will be important to include exemptions on grounds of national security, discharge of statutory functions, protection of health and safety of citizens and such other circumstances as appropriate. However, in articulating exceptions care must be taken to ensure that the purpose for framing of the legislation is not diluted so much as to make it meaningless. Thus, while national security exemptions are necessary and recommended, they should be framed carefully to ensure that it is not possible for just anyone to claim that the provisions of the law are not applicable by citing some national security interest without substantiation.

5.1.13 Regulatory Set Up

The data protection legislations analysed here has established a special regulator to deal with contraventions of the legislation as well as to more proactively supervise compliance with the statute. The regulator also prescribes the standards against which compliance is measured and is called upon to adjudicate disputes in relation to the provisions of the law.

The extent to which a data regulator is required in the context of Indian data protection legislation will depend to a large extent on the shape of the legislation. In the event it is intended that the law should operate as umbrella legislation under the terms of which various sector specific legislations would spell out the more detailed sector oriented issues, then a regulator would be required to harmonise the provisions of the data protection law with the sector specific legislations. Where the legislation spells out the broad principles for data protection, it will be left to the data regulator to articulate the specific regulations. There are 3 options regarding setting up a regulatory mechanism to enforce the law:

(a) Heavy handed Regulation through a separate regulator

(b) Light handed regulation through office of Ombudsman and reliance on self-regulation by government and industry bodies.

(c) Converting existing Information Commissions into privacy and information commissions who will enforce the legislative provisions.

The proposed Data Protection Legislation incorporates principles that form the basis of data protection of individuals both by the public authorities and private corporate, NGOs and other entities that collect data. It establishes Data Protection Authority with its headquarters at Delhi and other offices at almost all capital of every state of India and recognizes the role of organisation. The powers and duties of Authority are being set in the proposed legislation at length.

5.1.14 Comparison With The Personal Data Protection (Draft) Bill, 2018

In 2017 and 2018 status of protection in India was the focal point of numerous discourses. The presence of privacy as one of the fundamental right was confronted by the government before the Supreme Court. Promoters favoring privacy were viewed as differentiating the estimations of Indian culture. Endeavours for framing a separate legislation for data protection were in vein. The most recent judgment of Supreme Court on Aadhaar confronted the manner personal data is protected in India.

On 24 August 2017, a nine-judge bench of the Supreme Court laid down judgment, together upholding that privacy was a fundamental right, retaining individual's nobility and independence and expressing it as the core of the constitutional order. Privacy in this technologically advanced world is no more an extravagance concern; it influences each person as it is pervasive through the mode of web. By the end of July, Justice B. N. Shrikrishna Committee was appointed by the government who came up with a report along with a draft bill for data protection for India.

In spite of the fact that the Draft Bill For Personal Data Protection confined by Justice B. N. Shrikrishna Committee (hereafter referred as Draft

Bill) covers serious issues identified with personal data which needs protection, it has still left much hazy area which should be attended too. India is place where diverse languages are method of correspondence utilized by its nationals. There are numerous residents of India who even today has shallow comprehension of Hindi or English. The Draft Bill neglects to address this unpredictable circumstance. Aside from the conceivability of languages another issue that the Draft Bill neglected to address is the issue of lack of education. Huge populace of India is illiterate yet at the same time their data is collected, stored and processed by both government as well as private entities and there are no arrangements made tending to illiteracy.

The Bill suggested by the researcher is after research carried in various field. There are differences in the Draft Bill suggested by Justice B. N. Shrikrishna and the Bill suggested by the researcher. The researcher has taken care of the language understanding of the citizens of India which The Personal Data Protection Bill, 2018 has failed to address. Another issue which has been taken care of by the researcher in her Bill is illiteracy. The illiteracy rate is high in India and hence it cannot be avoided. For Aadhaar programme data of illiterate people is also collected in the same manner banks, mobile service providing companies and so on collects, store and process the data of illiterate people also. Thus a protection to their data is equally important and their consent for processing of data at the same time is also important. This issue has not been addressed by The Personal Data Protection Bill, 2018.

The researcher has laid the functions to be performed by the Adjudicating Officer which is clear to avoid ambiguity unlike The Personal Data Protection Bill, 2018. The researcher has also suggested notification clause for data managers which is governed by the Adjudicating Officer. This provision is added so that the Adjudicating Officer can know which data manager is processing what kind of data along with the details of data manager so that he cannot escape easily.

Notification by Data Managers is a chapter added to the Bill suggested by the researcher. This chapter obliges the data manager to make themselves register with the Adjudicating Officer. The notification by the data managers must have details particulars like his name, address and so on of the data manager along with details of the data being processed or the information of data which data manager intends to process. This gives the Adjudicating Officer a chance to have an eye on which data manager is processing what kind of data. This provision can minimize the incidents of data theft or fraud as the Adjudicating Officer would have the knowledge about what data is being processed.

Further the functioning of Data Protection Authority and its office establishment is not made clear in The Personal Data Protection Bill, 2018. However, the researcher has explained those clauses clearly. Further the Draft Bill of researcher has suggested ground level of redressal as every time moving to state tribunal for justice would be costly as well as time consuming for the one's who dwells far from the location of state tribunal. Ground level of redressal has been escaped by The Personal Data Protection Bill, 2018.

Further according to the survey carried out by researcher direct marketing calls, mails, sms, what's app and so on are nuisance to 70% of people who were samples for carrying out the research. 30% of the samples for carrying the research said that the Do Not Disturb application is inefficient as if one has registered with DND still they receive call, sms, etc from various companies. The researcher has made a special provision for direct marketing in her Draft Bill while The Personal Data Protection Bill, 2018 has not explicitly mentioned about direct marketing in whole Bill.

Grievance and Redressal is provided but is not explicit. The role of Adjudicating wing and Adjudicating Officer is not made clear. Moreover, ground level redressal is not clear. A proper system must be set up so that easy and cost effective redressal to the victim is provided. The Draft Bill provides provisions for redressal but proper distribution of the work is not explained in

the Draft Bill. The researcher has tried to suggest a law with covers large area of data for protection. Redressal system suggested by the research would solve the issues at district level. Due to this the state level and national level tribunal would not be overloaded with the petitions.

Direct marketing is the much utilized method of marketing in today's time. Indeed, even Banks, educational institutions, tuition classes, mobile companies, online shopping, small shops, eateries, salon, and so forth are utilizing direct marketing to approach their target audience. Direct marketing involves a direct approach to the target audience. This approach incorporates tele-promoting, SMS or mailing to the target audience. Direct marketing might be the most ideal approach to reach target audience, however from the target audience perspective the scene may be contrast. Direct marketing has increased to that extent that DO NOT DISTURB (DND) kind of services has to be initiated. The researcher went to the common people specially educated to get the answer that whether the direct marketing is helpful or is a aggravation. The consequences of the overview led by the researcher were that 70% of the public thought that direct marketing is an annoyance to them. The people involved in direct marketing, calls their target audience at any time hence, it creates nuisance for the people. 30% of people say that though they have registered with the DND service, despite everything they get promoting calls from various organizations. This serious issue has not been addressed by the Draft Bill. No explicit provision has been made for direct marketing. Direct Marketing is the result of lack of data protection. The approach to the target audience direct marketers makes is due to easy flow of data. Such companies collects the data from call centres, other institutions, and so on paying for the data and then use direct marketing to promote their product or service.

Further the penalty provided to data offender is just 2% of its annual worldwide gain which is not sufficient. Hence the penalty section must be revised and must be marked at such level that anyone needs to think twice before performing data theft or fraud.

6. CONCLUSION ABOUT THE RESEARCH

The research questions are answered throughout the thesis in order to meet the five research objectives set by the researcher. The Hypothesis stands correct framed by the researcher. The answers try to meet the expectations and hypothesis stand correct as per the present scenario of data protection in India.

7. SUGGESTED DRAFT BILL HERE ONWARDS

DATA PROTECTION DRAFT BILL, 2019

Table of Contents

Chapter IV Rights Of Data Subject

Chapter V Notifications By Data Managers

Chapter VI Obligations Of Data Managers

Chapter VII The Data Protection Authority

Chapter VIII Exemptions

Chapter IX Appellate Tribunal

Chapter X Offences And Penalties

Chapter XI MiscellaneousProvisions

Chapter I. Preliminary

1. Short title, extent and commencement

1. This Act may be called the Data Protection Act, 2018.
2. It extends to whole of India.
3. It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint.

2. Definitions

In this Act and in any rules made thereunder, unless the context otherwise requires, –

(a) "**appropriate government**" means, in relation the Central Government or a Union Territory Administration, the Central Government; in relation a State Government, that State Government; and, in relation to a public authority which is established, constituted, owned, controlled or substantially financed by funds provided directly or indirectly –

i. By the Central Government or a Union Territory Administration, the Central Government

ii. By a State Government, that State Government

(b) **"Authority"** means the Data Protection Authority of India established under Chapter VII of this Act;

(c) Basic "**Data**" means collection, compilation or representation of information, knowledge, facts, concepts or instructions which are prepared or have been prepared in a formalized manner and which –

i. Is being processed by means of equipment operating automatically including computer system or computer network in response to instructions given for that purpose,

ii. Is recorded with the intention that it should be processed by means of such equipment,

iii. Is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.

(d) "**Data Manager**" means, a person who (governmental or non-governmental; alone or jointly; in common or with other persons) determines the purposes for which and the manner in which any data are to be processed.

(e) "**Data Processor**", means any person (other than an employee of the data manager) who processes the data on behalf of the data manager;

(f) "**Data Subject**" means an individual whose data is processed by data manager;

(g) "**Personal Data**" means any information relating to an identified or identifiable living individual; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(h) "**Data Processing**", means obtaining, recording or holding the data or carrying out any operation or set of operations on the data, including—

i. Organisation, adaptation or alteration of the data,

ii. Retrieval, consultation or use of the data,

iii. Disclosure of the data by transmission, dissemination or otherwise making available, or

iv. alignment, combination, blocking, erasure or destruction of the data;

(i) "**relevant filing system**" means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

(j) "**Anonymise**" means, the removal of all data that may, whether directly or indirectly in conjunction with any other data, be used to identify the data subject

(k) "**Disclose**" means, any action or activity that results in a person who is not the data subject coming into the possession or control of that personal data;

(l) "**Destroy**" means, to cease the existence of, by deletion, erasure or otherwise, any personal data;

(m) "**collect**" means, any action or activity that results in a data manager obtaining, or coming into the possession or control of, any personal data of a data subject;

(n) "**Receive**" means, to come into the possession or control of any personal data;

(o) "**the special purposes**" means any one or more of the following—

a) the purposes of journalism,

(b) artistic purposes, and

(c) literary purposes.

(p) "**biometric data**" means any data relating to the physical, physiological or behavioural characteristics of a person which allow their unique identification including, but not restricted to, facial images, finger prints, hand prints, foot prints, iris recognition, hand writing, typing dynamics, gait analysis and speech recognition;

(q) **"Financial data"** means any number or other personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data subject or any personal data regarding the relationship between a financial institution and a data subject including financial status and credit history;

(r) **"Genetic data"** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the behavioral characteristics, physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(s) **"Health data"** means data related to the state of physical or mental health of the data subject and includes records regarding the past, present or future state of the health of such data subject, data collected in the course of registration for, or provision of health services, data associating the data subject to the provision of specific health services.

(t) **"Authentic identifier"** means any number, code, or other identifier, including Aadhaar number, assigned to a data subject under a law made by Parliament or any State Legislature which may be used for the purpose of verifying the identity of a data subject;

(u) **"Transgender status"** means the condition of a data subject whose sense of gender does not match with the gender assigned to that data subject at birth, whether or not they have undergone sex reassignment surgery, hormone therapy, laser therapy, or any other similar medical procedure.

(v) "Infringement or Violation" includes—

(i) bodily or mental injury;

(ii) loss, distortion or theft of identity;

(iii) financial loss or loss of property,

(iv) loss of reputation, or humiliation;

(v) loss of employment;

(vi) any discriminatory treatment;

(vii) any subjection to blackmail or extortion;

(viii) any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data subject;

(ix) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; or

(x) any observation or surveillance that is not reasonably expected by the data subject.

All other expressions used herein shall have the meanings ascribed to them under the General Clauses Act, 1897 (10 of 1897) or the Code of Criminal Procedure, 1973 (2 of 1974), as the case may be.

3. Sensitive personal data

In this act "sensitive personal data" means personal data consisting of information of the data subject as to—

a. The racial or ethnic origin;
b. Passwords;
c. Religious beliefs, political opinions or other beliefs/opinions of a similar nature;
d. Health data;
e. Sexual preferences and practices;
f. Authorized Identifiers;
g. The commission or alleged commission by him of any offence (kind of criminal record), or;
h. Transgender status;
i. Biometric data;
j. Genetic data along with the DNA sample;
k. Financial and credit information.

Chapter II Provision for protection of Data

4. "Valid Consent"

The consent must be explicit or non-explicit. However, valid consent is divided into following categories under this act-

i. Free and Clear Consent is consider valid when the data subject exercises a real choice and there is no risk of deception, intimidation,

coercion or significant negative consequences if he/she does not consent;

ii. Informed Consent is a precise, easy and clear description of the subject matter requiring consent and, further, outline the consequences of consenting or not consenting, (language used for information must be understandable to the data subject, use of local language is more preferable in rural areas, in case of illiterate data subject information must be explained to him for consent);

iii. Specific Consent, consent must also be specific with reference to the quality of information given about the object or purpose for taking consent; and

iv. Withdrawal Of Consent, data subject can withdraw his consent at any point of time with ease.

5. Collection Of Data

i. No data of a data subject shall be collected except in conformity with section 6 and section 7;

ii. No personal data or sensitive personal data of a data subject may be collected under this Act unless it is essential for the attainment of a purpose of the person seeking its collection;

iii. Subject to section 6 and section 7, no data may be collected under this Act before giving notice in the prescribed manner laid down for collection to the data subject.

6. Collection Of Data With Prior Informed Consent

a. Subject to sub-section (b) of this section, a person pursuing to collect data under this section shall, prior to its collection, obtain the consent of the data subject.

b. Prior to a collection of data under this section, the person seeking its collection shall inform the data subject of the following details in respect of his personal data, namely: –

   i. when it shall be collected
   ii. its content and nature
   iii. the purpose of its collection
   iv. the manner in which it may be accessed, checked and modified
   v. the security practices, privacy policies and other policies, if any, to which it will be subject
   vi. the conditions and manner of its disclosure
   vii. the procedure for recourse in case of any grievance in relation to it

c. Consent to the collection of data under this section may be obtained from the data subject in any manner or medium but shall not be obtained as a result of a threat, duress or coercion: Provided that the data subject may, at any time after his consent to the collection of data has been obtained, withdraw the consent for any reason whatsoever and all data collected following the original grant of consent shall be destroyed forthwith.

7. Collection Of Data Without Prior Consent

Data may be collected without the prior consent of the data subject if it is –

a. necessary for the provision of an emergency medical service to the data subject;
b. required for the establishment of the identity of the data subject and the collection is authorised by a law in this regard;
c. necessary to prevent a reasonable threat to national security, defence or public order;
d. necessary to prevent, investigate or prosecute a cognisable offence.

8. Storage Limitation of data

a. No person shall store any data for a period longer than it is necessary to achieve the purpose for which it was collected or received, or, if that purpose is achieved or ceases to exist for any reason, for any period following such achievement or cessation.

b. Save as provided in sub-section (c), any data collected or received in relation to the achievement of a purpose shall, if that purpose is achieved or ceases to exist for any reason, be destroyed forthwith.

c. Notwithstanding anything contained in this section, any data may be stored for a period longer than is necessary to achieve the purpose for which it was collected or received, or, if that purpose has been achieved or ceases to exist for any reason, for any period following such achievement or cessation, if –

   i. the data subject grants his consent to such storage prior to the purpose for which it was collected or received being achieved or ceasing to exist

   ii. it is adduced for an evidentiary purpose in a legal proceeding

   iii. it is required to be stored under the provisions of an Act of Parliament Provided that only that amount of personal data that is necessary to achieve the purpose of storage under this sub-section shall be stored and any personal data that is not required to be stored for such purpose shall be destroyed forthwith, Provided further that any personal data stored under this sub-section shall, to the extent possible, be anonymised.

9. Processing of data

a. Such data shall not be processed which is not necessary for the achievement of the purpose for which it was collected or received.

b. No data shall be processed for any purpose other than the purpose for which it was collected or received.

c. Personal data may be processed on the basis of the valid consent of the data subject, given no later than at the commencement of the processing.

d. Processing of personal data for employment purpose:- Processing of personal data may be considered legal if such processing is necessary for—

(1) recruitment or dismissal of employment of a data subject by the data manager;

(2) any service benefit or other benefits provided during employment to the data subject who is employee of the data manager;

(3) authenticating attendance of the data subject who is an employee of the data manager; or

(4) the valuation of performance of data subject being employee of data manager.

e. Processing of data for reasonable purposes.**:-** Notwithstanding anything contained in this section, any data may be processed for a purpose other than the purpose for which it was collected or received if –

i. the data subject grants his consent for processing;

ii. it is necessary to perform a contractual duty to the data subject;

iii. it is necessary to prevent a reasonable threat to national security defence or public order;

iv. it is necessary for functions of Parliament and State Legislature;

v. it is necessary for compliance of law made by Parliament or State Legislature;

vi. it is necessary for compliance of order or judgement given by any court or tribunal of India;

vii. it is necessary to prevent, investigate or prosecute a cognisable offence;

viii. it is necessary for medical emergency threatening to the life of data subject, any other individual or public at large;

ix. it is necessary to provide medical treatment during epidemic to data subject, other individual or public at large;
x. it is necessary for ensuring safety and assistance to the data subject during disaster like situations and public disorder;
xi. it is necessary for mergers and acquisitions;
xii. it is necessary for network and information security;
xiii. it is necessary for credit scoring;
xiv. it is necessary for recovery of debt;
xv. it is necessary for processing of publicly available personal data;

10. Notice.—

a. The data manager shall provide the data subject with the following information, no later than at the time of collection of the personal data or, if the data is not collected from the data subject, as soon as is reasonably practicable—

i. the purposes for which the personal data is to be processed;
ii. the categories of personal data being collected;
iii. the identity and contact details of the data manager and the contact details of the data protection supervisor, if applicable;
iv. the right of the data subject to withdraw such consent, and the procedure for such withdrawal, if the personal data is intended to be processed on the basis of consent;
v. the basis for such processing, and the consequences of the failure to provide such personal data, if the processing of the personal data is based on the grounds in section 9, and section 9 (d);
vi. the source of such collection, if the personal data is not collected from the data subject;

vii. the individuals or entities including other data managers or data processors, with whom such personal data may be shared, if applicable;

viii. information regarding any cross-border transfer of the personal data that the data manager intends to carry out, if applicable;

ix. the period for which the personal data will be retained in terms of section 8 or where such period is not known, the criteria for determining such period;

x. the existence of and procedure for the exercise of data subject's rights mentioned in Chapter IV and any related contact details for the same;

xi. the procedure for grievance redressal under section 44;

xii. the existence of a right to file complaints to the Authority;

xiii. where applicable, any rating in the form of a data trust score that may be assigned to the data manager under section 40; and

xiv. any other information as may be specified by the Authority.

b. The data manager shall provide the information as required under this section to the data subject in a clear and concise manner that is easily comprehensible to a reasonable person and in multiple languages where necessary and practicable.

c. Sub-section (a) shall not apply where the provision of notice under this section would substantially prejudice the purpose of processing of personal data under sections 9 (a) to (c) or section 16 (f) of this Act.

11. Transfer Of Data For Processing

a. Subject to the provisions of this section, data that has been collected in conformity with this Act may be transferred by a data manager to a data

processor, whether located in India or otherwise, if the transfer is pursuant to an agreement that explicitly binds the data processor to same or stronger measures in respect of the storage, processing, destruction, disclosure and other handling of the personal data as are contained in this Act.

b. No data processor shall process any data transferred under this section except to achieve the purpose for which it was collected.

c. A data manager that transfers data under this section shall remain liable to the data subject for the actions of the data processor.

12. Trans-border flow of Personal Data

No data manager shall transfer any personal data relating to data subject outside the territory of India unless:

a. the recipient of the personal data is subject to a law, code of conduct or contract which binds such recipients;
b. the Central Government, after consultation with the Authority, has permitted transfer of data to a particular country, or to a sector within a country or to a particular international organization; or
c. the Authority permits a particular transfer or set of transfers of data due to a demand of situation; or
d. the data subject has given consent for the transfer of data after being satisfied with the conditions laid down in clause (a) or (b); or
e. the data subject has explicitly consented for the transfer of information categorized under sensitive personal data after being satisfied with the conditions laid down in clause (a) or (b).

13. Security Of Data And Onus Of Confidentiality

a. No person shall collect, receive, store, process or otherwise handle any data without implementing measures, including, but not restricted to,

technological, physical and administrative measures, adequate to secure its confidentiality, secrecy, integrity and safety, including from theft, loss, damage or destruction.

b. Data managers and data processors shall be subject to a duty of confidentiality and secrecy in respect of data in their possession or control.

c. Without prejudice to the provisions of this section, a data manager or data processor shall, if the confidentiality, secrecy, integrity or safety of data in its possession or control is violated by theft, loss, damage or destruction, or as a result of any disclosure contrary to the provisions of this Act, or for any other reason whatsoever, notify the data subject, in such form and manner as may be prescribed under this Act.

14. Disclosure of data

No person shall disclose, or otherwise cause any other person to receive, the content or nature of any data that has been collected in conformity with this Act.

a. Disclosure of data with prior informed consent

i. Subject to sub-section (ii), a data manager or data processor seeking to disclose data under this section shall, prior to its disclosure, obtain the consent of the data subject.

ii. Prior to a disclosure of data under this section, the data manager or data processor, as the case may be, seeking to disclose the data, shall inform the data subject of the following details in respect of his data, namely: –

1. when it will be disclosed;
2. the purpose of its disclosure;
3. the security practices, privacy policies and other policies, if any, that will protect it; and

4. the procedure for recourse in case of any grievance in relation to it.

b. Disclosure of data without prior consent

i. Subject to sub-section (ii), data may be disclosed without the prior consent of the data subject if it is necessary –
   a. to prevent a reasonable threat to national security, defense or public order
   b. to prevent, investigate or prosecute a cognizable offence

ii. No data manager or data processor shall disclose any data unless it has received an order in writing from a police officer not below the rank of Deputy Commissioner in such form and manner as may be prescribed:

   1. Provided that an order for the disclosure of data made under this sub-section shall not require the disclosure of any data that is not necessary to achieve the purpose for which the disclosure is sought;
   2. Provided further that the data subject shall be notified, in such form and manner as may be prescribed, of the disclosure of his data, including details of its content and nature, and the identity of the police officer who ordered its disclosure, forthwith.

15. Exactitude Of Personal Data

a. Each data manager and data processor shall, ensure that the personal data in its possession, is accurate and, where necessary, is kept up to date.

b. No data manager or data processor shall deny a data subject whose personal data is in its possession, the opportunity to review his

personal data and, where necessary, rectify anything that is inaccurate or not up to date.

c. A data subject may, if he finds personal data in the possession of a data manager or data processor that is not necessary to achieve the purpose for which it was collected, received or stored, demand its destruction, and the data manager shall destroy, or cause the destruction of, the personal data forthwith.

16. Special provisions for sensitive personal data

a. Consent

Valid explicit consent is mandatory for processing Sensitive Personal Data. All the three conditions laid down under section 4 of this Act for valid consent must be satisfied i.e., consent must be free and clear, data subject must be well informed about the purposes of processing his data along with the consequences and lastly specific consent with regard to whether the data subject is given the choice to consent separately for the purposes of processing different categories of sensitive personal data relevant.

b. Storage

No person shall store sensitive personal data for a period longer than is necessary to achieve the purpose for which it was collected or received, or, if that purpose has been achieved or ceases to exist for any reason, for any period following such achievement or cessation.

c. Processing

No person shall process sensitive personal data for a purpose other than the purpose for which it was collected or received.

d. Disclosure

No person shall disclose sensitive personal data to another person, or otherwise cause any other person to come into the possession or control of, the content or nature of any sensitive personal data, including any other details in respect thereof.

e. Exemptions

Sensitive personal data may be processed if such processing is strictly necessary for:

1. Parliament or State Legislature functioning;
2. the exercise of any function of the State authorized by law for the provision of any service or benefit to the data subject.
3. explicitly mandated under any law made by Parliament or any State Legislature; or
4. necessary for compliance with any order or judgment given by any Court or Tribunal in India.

f. Circumstantial Processing Of Sensitive Personal Data —

Certain categories of sensitive personal data such as passwords, financial data, health data, authorized identifiers, genetic data, and biometric data may be processed where such processing is inevitable. Such circumstances are as follows —

i. for any medical emergency dangerous for the life or health of the data subject; or
ii. in situations of epidemic or threat to public health at large data subject's health data can be processed to provide appropriate treatment to him; or

g. in case of any calamity or public disorder, sensitive personal data shall be processed to provide security and support to the data subject.

h. Further categories of sensitive personal data.

i. Such further categories of personal data as may be specified by the Authority shall be sensitive personal data and, where such categories of personal data have been specified, the Authority may also specify any further grounds on which such specified categories of personal data may be processed.

ii. The Authority shall specify categories of personal data under sub-section (i) having regard to—

1. the risk of significant harm that may be caused to the data subject by the processing of such category of personal data;
2. the expectation of confidentiality attached to such category of personal data;
3. whether a significantly discernible class of data subjects may suffer significant harm from the processing of such category of personal data; and
4. the adequacy of protection afforded by ordinary provisions applicable to personal data.

iii. The Authority may also specify categories of personal data, which require additional safeguards or restrictions where repeated, continuous or systematic collection for the purposes of profiling takes place and, where such categories of personal data have been specified, the Authority may also specify such additional safeguards or restrictions applicable to such processing.

Chapter III PERSONAL AND SENSITIVE PERSONAL DATA OF CHILDREN

17. Processing Of Personal Data And Sensitive Personal Data Of Children. —

a. Personal data of children shall be processed by data manager with utmost safeguards which may protect as well as develop the rights and benefits to the child.

b. Adequate measures for age authentication and parental consent shall be included by data managers in order to process personal data of children.

c. Adequate measures for age authentication included by a data manager shall be considered on the basis of—

   i. quantity of personal data processed;

   ii. proportion of such personal data likely to be that of children;

   iii. probability of risk to children resulting out of processing of personal data; and

      i. such other factors as may be specified by the Authority.

d. The Authority shall notify the following as guardian data managers—

   i. data managers who operate commercial websites or online services directed at children; or

   ii. data managers who process large quantity of personal data of children.

e. Guardian data managers shall be barred from profiling, tracking, or behavioral monitoring of, or targeted advertising directed at children and undertaking any other processing of personal data that can cause significant detriment to the child.

f. Sub-section (e) may apply in such modified form, to data managers offering counseling or child protection services to a child, as the Authority may specify.

g. Where a guardian data manager notified under sub-section (d) exclusively provides counseling or child protection services to a child, as under sub-section (f), then such guardian data manager will not be required to obtain parental consent as set out under sub-section (b).

Chapter IV Rights of Data subject

Every individual or data subject shall have the right under national law to request from any data manager information as to whether the data manager is processing his or her data. However, such data subject must produce relevant identity proof while requesting access to personal data. Data subjects shall have the right under this Act to:

18. Access To Own Personal Data

This includes the set of rights which are as follows:

a. To be informed by any data manager whether personal data of which that individual is the data subject are being processed by or on behalf of that data manager,

b. If that is the case, to be given by the data manager a description of,
   i. the personal data of which that individual is the data subject;
   ii. the purposes for which they are being or are to be processed;
   iii. the recipients or classes of recipients to whom they are or may be disclosed.

c. To have communicated to him in an intelligible form,
   i. the information constituting any personal data of which that individual is the data subject;

ii. any information available to the data manager as to the source of those data.

Explanation: Here intelligible form refers to the language known by the data subject. For example where the data subject is not well conversant with Hindi or English, he must be communicated with the information about his data in the local or vernacular language by the data manager.

d. In case where the data subject is illiterate the information of his data must be explained to him verbally before a witness and thumb impression of such data subject must be considered as consent. An acknowledgement letter must be provided by the data subject along with the signature of the witness and the thumb impression of the data subject after understanding the information given by the data manager. Or a video recording done by the data manager giving the information to the illiterate data subject can also be considered as valid according to this Act.

Explanation: this provision has been inserted in the Act keeping in mind the illiteracy rate in India. An illiterate individual can also be victimized by data theft or fraud.

e. Where the processing by automatic means of personal data of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him, to be informed by the data manager of the logic involved in that decision-taking.

f. Where a data manager cannot comply with the request without disclosing information relating to another individual who can be identified from that information, he is not obliged to comply with the request unless—

i. the other individual has consented to the disclosure of the information to the person making the request, or
ii. it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

g. In determining for the purposes of subsection (f)(ii) whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned, regard shall be had, in particular, to—

i. any duty of confidentiality owed to the other individual;
ii. any steps taken by the data manager with a view to seeking the consent of the other individual;
iii. whether the other individual is capable of giving consent, and
iv. any express refusal of consent by the other individual.

19. Rectification, Erasure And Blocking Of Data

a. Under this provision, data subjects have the right to obtain from the manager the rectification, erasure or blocking of their data if they think that their processing does not comply with the provision of this Act, in particular because of the imperfect or incomplete nature of the data.
b. A data subject's request to erase or delete any data is often based on a claim that the data processing does not have a legitimate basis. Such claims often arise where consent has been withdrawn, or where certain data are no longer needed to execute the purpose of the data collection. Under such circumstance the data subject can request to delete the data.
c. According to the ideology of accountability, the manager must at any time be able to exhibit that there is a sound legal basis to its

data processing; otherwise the processing must be stopped. If the processing of data is contested because the data are allegedly incorrect or unlawfully processed, the data subject, in accordance with the ideology of fair processing, can demand that the data under dispute be blocked. This means that the data are not deleted but that the manager must refrain from using the data during the period of blockage.

d. Data subjects additionally have the right to obtain from the manager the notification to third parties of any blocking, rectification or erasure, if they had received data prior to these processing operations. As the disclosure of data to third parties ought to have been documented by the manager, it should be possible to identify the data recipients and request deletion.

e. The legal heirs, guardians and authorised representatives of the data subject has a right to request for the deletion of the data of the data subject on producing legal proof in case of death of such data subject. Such data subject ceases to be a natural person and therefore is no longer protected under the statute.

20. Objection

Right to object about the processing of their data if it leads to disproportionate results,

i. Data subject is empowered under this Act, to raise objection on compelling legitimate grounds relating to the data subject's particular situation which may lead to disproportionate results. Such provisions aim at finding the correct balance between the data subject's data protection rights and the legitimate rights of others in processing the data subject's data

ii. The effect of a successful objection is that the data in question may no longer be processed by the manager. Processing operations performed on the data subject's data prior to the objection, however, remain legitimate.

21. Object Further Use Of Data For Direct Marketing Purposes

This provides provisions for a precise right to object to the use of one's data for the purposes of direct marketing. This kind of objection is meant to be raised before data are made available to third parties for the purpose of direct marketing. The data subject must, therefore, be given the opportunity to object before the data are transferred.

22. Right to Restrict.

a. The data subject shall have the right to restrict continuing disclosure of personal data by a data manager related to the data subject where such disclosure—

   i. has served the purpose for which it was made or is no longer necessary;
   ii. was made on the basis of consent under section 9(c) and such consent has since been withdrawn; or
   iii. was made contrary to the provisions of this Act or any other law made by Parliament or any State Legislature.

b. Sub-section (a) shall only apply where the Adjudicating Officer under section 61 determines the applicability of clause (i), (ii) or (iii) of sub-section (a) and that the rights and interests of the data subject in preventing or restricting the continued disclosure of personal data

override the right to freedom of speech and expression and the right to information of any citizen.

c. In determining whether the condition in sub-section (b) is satisfied, the Adjudicating Officer shall have regard to—

i. the sensitivity of the personal data;
ii. the scale of disclosure and the degree of accessibility sought to be restricted or prevented;
iii. the role of the data subject in public life;
iv. the relevance of the personal data to the public; and the nature of the disclosure and of the activities of the data manager, particularly whether the data manager systematically facilitates access to personal data and whether the activities would be significantly impeded if disclosures of the relevant nature were to be restricted or prevented.

d. The right under sub-section (a) shall be exercised by filing an application in such form and manner as may be prescribed.

e. Where any person finds that personal data, the disclosure of which has been restricted or prevented by an order of the Adjudicating Officer under sub-section (b) does not satisfy the conditions referred to in that sub-section any longer, they may apply for the review of that order to the Adjudicating Officer in such manner as may be prescribed, and such Adjudicating Officer shall review her order on the basis of the considerations referred to in sub-section (c).

23. Provisions For Credit Information Company

a. Where the data manager is a credit information company, section 18 has effect subject to the provisions of this section.

b. An individual making a request under section 18 may limit his credit reference request to personal data relevant to his financial standing, and shall be agency taken to have so limited his request unless the request shows a contrary intention.

c. Where the data manager receives a request under section 18 in a case where personal data of which the individual making the request is the data subject are being processed by or on behalf of the data manager, the obligation to supply information under that section includes an obligation to give the individual making the request a statement, in such form as may be prescribed by the regulations laid under the Credit Information Companies (Regulations) Act, 2005.

24. Standard Conditions for Exercising The Above Rights—

a. Any request for exercising the rights granted under Chapter IV by the data subject must be made in writing to the data manager along with reasonable information necessary for the identity of the data subject to satisfy the data manager . The data manager shall acknowledge receipt of such request within such period of time as may be specified.

b. Prescribed fee must be paid along with the request made by the data subject.

c. Data manager should comply with the request made by the data subject within reasonable time as specified by the authority along with the acknowledgment referred in sub-section (a).

d. In case where data manger refuses to comply with the request of data subject, such refusal should be accompanied with adequate reasons in writing. At the same time data subject must be informed about his right to

complaint with the Authority against the refusal within a prescribed period of time and manner.

e. When the question of damage to other's rights is involved, the data manager is not obliged to comply with any request made under this Chapter where such compliance would harm the rights of any other data subject under this Act.

f. The manner of exercise of rights under this Chapter shall be in such form as may be provided by law or in the absence of such law, in a reasonable format to be followed by each data manager.

Chapter V Notifications By Data Managers

25. The Particulars To Be Provided By Data Manager

a. Registrable Particulars

1. His name and address of the data subject,
2. Explanation of the personal data being or to be processed by or on behalf of the data manager and of the category or categories of data subject to which they relate,
3. Explanation of the purpose or purposes for which the data are being or to be processed,
4. Explanation of any recipient or recipients to whom the data manager intends or may wish to disclose the data,
5. Declaration of the names of countries outside India to which the data manager directly or indirectly transfers, or intends directly or indirectly to transfer.

b. Regulations

1. "fees regulations" means regulations made by the Central Government under section 33;

2. "notification regulations" means regulations made by the central government under section 32 of this Act;
3. "Prescribed", except where used in relation to fees regulations, means prescribed by notification regulations.

c. Address

For the purposes of this Part, so far as it relates to the addresses of data managers—

1. the address of a registered company is that of its registered office
2. the address of a person (other than a registered company) carrying on a business is that of his subject place of business in India

26.Restriction On Processing Data Without Registration

a. Subject to the following provisions of this section, personal data must not be processed unless an entry in respect of the data manager is included in the register maintained by the Adjudicating Officer under section 25 (or is treated by notification regulations made by virtue of section 25(c) as being so included).
b. If it appears to the Adjudicating Officer that processing of a particular description is unlikely to prejudice the rights and freedoms of data subjects, notification regulations may provide that, in such cases as may be prescribed, subsection (a) is not to apply in relation to processing of that description.
c. Subsection (a) does not apply in relation to any processing whose sole purpose is the maintenance of a public register.

27. Notification By Data Managers

a. Any data manager who wishes to be included in the register maintained under section 28 shall give a notification to the Adjudicating Officer under this section.

b. A notification under this section must specify in accordance with notification regulations—

   i. the registrable particulars

   ii. a general description of measures to be taken for the purpose of appropriate technical and organisational dealings taken against unauthorised or unlawful processing of data and against accidental loss or destruction of, or damage to data

c. Notification regulations may make provision as to the giving of notifications,

   i. by partnerships, or

   ii. in other cases where two or more persons are the data managers in respect of any personal data

d. The notification must be accompanied by such fee as may be prescribed by fees regulations.

28. Register Of Notifications

a. The Adjudicating Officer shall maintain a register of persons who have given notification under section 25, and make an entry in the register in pursuance of each notification received by him.

b. Each entry in the register shall consist of—the registrable particulars notified under section 25 or, as the case requires, and such other information as the Adjudicating Officer may be authorised or required by notification regulations issued time to time by data protection authority to include in the register.

c. No entry shall be retained in the register for more than the relevant time except on payment of such fee as may be prescribed by fees regulations.

d. In subsection (c) "the relevant time" means twelve months or such other period as may be prescribed by notification regulations; and different periods may be prescribed in relation to different cases.

e. The Adjudicating Officer—

Shall provide facilities for making the information contained in the entries in the register available for inspection (in visible and legible form) by members of the public at all reasonable hours and free of charge;

Shall also provide such other facilities for making the information contained in those entries available to the public free of charge.

f. The Adjudicating Officer shall, on payment of such fee, if any, as may be prescribed by fees regulations, supply any member of the public with a duly certified copy in writing of the particulars contained in any entry made in the register.

29.Duty to Notify Changes

a. Notification regulations shall impose provision on every person in respect of whom an entry as a data manager included in the register maintained under section 27, a duty to notify any kind of changes to the Adjudicating Officer. The purpose referred here is that of ensuring at any time—

the entries in the register maintained under section 27 contain current names and addresses and describe the current practice or intentions of the data manager with respect to the processing of personal data, and Adjudicating Officer is provided with a general description of measures currently being taken as mentioned in section 27(b) (ii).

b. On receiving any notification for changes under notification regulations made by virtue of subsection (a) under this section, the Adjudicating Officer shall make such amendments of the relevant entry in the register maintained under section 27 as are necessary to take account of the notification.

30. Assessment by the Adjudicating Officer

a. In this section "assessable processing" means processing which is of a description specified in an order made by the Central Government as appearing to him to be particularly likely—
    1. to cause substantial damage or substantial distress to data subjects or,
    2. otherwise significantly to prejudice the rights and freedoms of data subjects

b. On receiving notification from any data manager under section 27 or under notification regulations made by virtue of section 32 the Adjudicating Officer shall consider—
    i. whether any of the processing to which the notification relates is assessable processing, and
    ii. if so, whether the assessable processing is likely to comply with the provisions of this Act

c. Subject to subsection (d) under this section, the Adjudicating Officer shall, within the period of 28 days beginning with the day on which he receives a notification which relates to assessable processing, give a notice to the data manager stating the extent to which the Adjudicating Officer is of the opinion that the processing is likely or unlikely to comply with the provisions of this Act.

d. Before the end of the period referred to in subsection (c) the Adjudicating Officer may, by reason of special circumstances, extend that period on one

occasion only by notice to the data manager by such further period not exceeding fourteen days as the Adjudicating Officer may specify in the notice.

e. No assessable processing in respect of which a notification has been given to the Adjudicating Officer as mentioned in subsection (b) shall be carried on unless either—
    i. the period of twenty-eight days beginning with the day on which the notification is received by the Adjudicating Officer (or, in a case falling within subsection (d), that period as extended under that subsection) has lapsed, or
    ii. before the end of that period (or that period as so extended) the data manager has received a notice from the Adjudicating Officer under subsection (c) in respect of the processing

31.Power to Appoint Data Protection Supervisor

a. The Adjudicating Officer may by order—
    i. make provision under which a data manager may appoint a person to act as a data protection supervisor responsible in particular for monitoring in an independent manner the data manager's compliance with the provisions of this Act, and
    ii. Provide that, in relation to any data manager who has appointed a data protection supervisor in accordance with the provisions of the order and who complies with such conditions as may be specified in the order, the provisions of this Part are to have effect subject to such exemptions or other modifications as may be specified in the order.
b. An order under this section may—
    i. Impose duties on data protection supervisors in relation to the Adjudicating Officer, and
    ii. Confer functions on the Adjudicating Officer in relation to data protection supervisors.

32.Function of Adjudicating Officer while making Notification Regulations

a. As soon as practicable after the passing of this Act, the Adjudicating Officer shall submit to the Authority appointed by Central Government proposals as to the provisions to be included in the first notification regulations.

b. The Adjudicating Officer shall keep under review the working of notification regulations and may from time to time submit to the Authority appointed by Central Government proposals as to amendments to be made to the regulations.

c. The Authority appointed by Central Government may from time to time require the Adjudicating Officer to consider any matter relating to notification regulations and to submit to him proposals as to amendments to be made to the regulations in connection with that matter.

d. Before making any notification regulations, the Authority appointed by Central Government shall consider any proposals made to him by the Adjudicating Officer under subsection (a), (b) or (c), and consult the Adjudicating Officer.

33.Fees Regulations

Fees regulations prescribing fees for the purposes of any provision of this Part may provide for different fees to be payable in different cases. In making any fees regulations, the Central Government shall have regard to the desirability of securing that the fees payable to the Adjudicating Officer are sufficient to offset the expenses incurred by the Adjudicating Officer and the Tribunal in discharging their functions and any expenses of the Central Government in respect of the Adjudicating Officer or the Tribunal.

Chapter VI Obligations Of Data Manager

34. Safeguarding Data Through Organizational Practices.

Every data manager shall implement policies and measures to ensure that—

(a) managerial, organizational, business practices and technical systems are designed in a manner to anticipate, identify and avoid harm to the data subject;

(b) the obligations mentioned in Chapter II are embedded in organizational and business practices;

(c) technology used in the processing of personal data is in accordance with commercially accepted or certified standards;

(d) legitimate interests of businesses including any innovation are achieved without compromising privacy interests;

(e) privacy is protected throughout processing from the point of collection to deletion of personal data;

(f) processing of personal data is carried out in a transparent manner; and

(g) the interest of the data subject is accounted for at every stage of processing of personal data.

35. Transparency.

a. The data manager shall take reasonable steps to maintain transparency regarding its general practices related to processing personal data and shall make the following information available in an easily accessible form as may be specified—

   i. the categories of personal data generally collected and the manner of such collection;
   ii. the purposes for which personal data is generally processed;

iii. any categories of personal data processed in exceptional situations or any exceptional purposes of processing that create a risk of significant harm;

iv. the existence of and procedure for the exercise of data subject rights mentioned in Chapter IV, and any related contact details for the same;

v. the existence of a right to file complaints to the Authority;

vi. where applicable, any rating in the form of a data trust score that may be accorded to the data manager under section 35;

vii. where applicable, information regarding cross-border transfers of personal data that the data manager generally carries out; and

viii. any other information as may be specified by the Authority.

b. The data manager shall notify the data subject of important operations in the processing of personal data related to the data subject through periodic notifications in such manner as may be specified.

36. Safeguards.

a. Having regard to the nature, scope and purpose of processing personal data undertaken, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, the data manager and the data processor shall implement appropriate security safeguards including—

i. use of methods such as anonymization and encryption;

ii. steps necessary to protect the integrity of personal data; and

iii. steps necessary to prevent misuse, unauthorized access to, modification, disclosure or destruction of personal data.

b. Every data manager and data processor shall undertake a review of its security safeguards periodically as may be specified and may take appropriate measures accordingly.

37. Data Breach.

a. The data manager shall notify the Authority of any personal data breach relating to any personal data processed by the data manager where such breach is likely to cause harm to any data subject.

b. The notification referred to in sub-section (a) shall include the following particulars—

   i. nature of personal data which is the subject matter of the breach;

   ii. number of data subjects affected by the breach;

   iii. possible consequences of the breach; and

   iv. measures being taken by the data manager to remedy the breach.

c. The notification referred to in sub-section (a) shall be made by the data manager to the Authority as soon as possible and not later than the time period specified by the Authority, following the breach after accounting for any time that may be required to adopt any urgent measures to remedy the breach or mitigate any immediate harm.

d. Where it is not possible to provide all the information as set out in sub-section (b) at the same time, the data manager shall provide such information to the Authority in phases without undue delay.

e. Upon receipt of notification, the Authority shall determine whether such breach should be reported by the data manager to the data subject, taking into account the severity of the harm that may be caused to such data subject or whether some action is required on the part of the data subject to mitigate such harm.

f. The Authority, may in addition to requiring the data manager to report the personal data breach to the data subject under sub-section (e), direct the data manager to take appropriate remedial action as soon as possible

and to conspicuously post the details of the personal data breach on its website.

g. The Authority may, in addition, also post the details of the personal data breach on its own website.

38. Data Protection Impact Assessment.

a. Where the data manager intends to undertake any processing involving new technologies or large scale profiling or use of sensitive personal data such as genetic data or biometric data, or any other processing which carries a risk of significant harm to data subjects, such processing shall not be commenced unless the data manager has undertaken a data protection impact assessment in accordance with the provisions of this section.

b. The Authority may, in addition, specify those circumstances, or classes of data manager, or processing operations where such data protection impact assessment shall be mandatory, and may also specify those instances where a data auditor under this Act shall be engaged by the data manager to undertake a data protection impact assessment.

c. A data protection impact assessment shall contain, at a minimum—

   i. detailed description of the proposed processing operation, the purpose of processing and the nature of personal data being processed;
   ii. assessment of the potential harm that may be caused to the data subjects whose personal data is proposed to be processed; and
   iii. measures for managing, minimizing, mitigating or removing such risk of harm.

d. Upon completion of the data protection impact assessment, the data protection supervisor shall review the assessment prepared and shall submit the same to the Authority in such manner as may be specified.

e. On receipt of the assessment, if the Authority has reason to believe that the processing is likely to cause harm to the data subjects, the Authority may direct the data manager to cease such processing or direct that such processing shall be subject to such conditions as may be issued by the Authority.

39. Maintaining The Records.

a. The data manager shall maintain accurate and up-to-date records of the following—

   i. important operations in the data life-cycle including collection, transfers, and erasure of personal data to demonstrate compliance as required under section 45;
   ii. periodic review of security safeguards under section 36;
   iii. data protection impact assessments under section 38; and
   iv. any other aspect of processing as may be specified by the Authority.

b. The records in sub-section (a) shall be maintained in such form as specified by the Authority.

c. Notwithstanding anything contained in this Act, this section shall apply to the Central or State Government, departments of the Central and State Government, and any agency instrumentality or authority which is "the State" under Article 12 of the Constitution.

40. Data Audits. —

a. The data manager shall have its policies and the conduct of its processing of personal data audited annually by an independent data auditor under this Act.

b. The data auditor will evaluate the compliance of the data manager with the provisions of this Act, including—

   i. clarity and effectiveness of notices under section 10;
   ii. effectiveness of measures adopted under section 34;
   iii. transparency in relation to processing activities under section 35;
   iv. security safeguards adopted pursuant to section 36;
   v. instances of personal data breach and response of the data manager, including the promptness of notification to the Authority under section 37; and
   vi. any other matter as may be specified.

c. The Authority shall specify the form, manner and procedure for conducting audits under this section including any civil penalties on data auditors for negligence.

d. The Authority shall register persons with expertise in the area of information technology, computer systems, data science, data protection or privacy, with such qualifications, experience and eligibility having regard to factors such as independence, integrity and ability, as it may specify, as data auditors under this Act.

e. A data auditor may assign a rating in the form of a data trust score to the data manager pursuant to a data audit conducted under this section.

f. The Authority shall specify the criteria for assigning a rating in the form of a data trust score having regard to the factors mentioned in sub-section (b).

g. Notwithstanding sub-section (a) where the Authority is of the view that the data manager is processing personal data in a manner that is likely to cause harm to a data subject, the Authority may order the data manager to conduct an audit and shall appoint a data auditor for that purpose.

41. Data Protection Supervisor. —

a. The data manager shall appoint a data protection supervisor for carrying out the following functions—

i. providing information and advice to the data manager on matters relating to fulfilling its obligations under this Act;

ii. monitoring personal data processing activities of the data manager to ensure that such processing does not violate the provisions of this Act;

iii. providing advice to the data manager where required on the manner in which data protection impact assessments must be carried out, and carry out the review of such assessment as under sub-section (d) of section 38;

iv. providing advice to the data manager, where required on the manner in which internal mechanisms may be developed in order to satisfy the principles set out under section 34;

v. providing assistance to and cooperating with the Authority on matters of compliance of the data manager with provisions under this Act;

vi. act as the point of contact for the data subject for the purpose of raising grievances to the data manager pursuant to section 44 of this Act; and

vii. maintaining an inventory of all records maintained by the data manager pursuant to section 39.

b. Nothing shall prevent the data manager from assigning any other function to the data protection supervisor, which it may consider necessary, in addition to the functions provided in sub-section (a) above.

c. The data protection supervisor shall meet the eligibility and qualification requirements to carry out its functions under sub-section (a) as may be specified.

d. Where any data manager not present within the territory of India carries on processing to which the Act applies, and the data manager is required to appoint a data protection supervisor under this Act, the data manager shall appoint such officer who shall be based in India and shall represent the data manager in compliance of obligations under this Act.

42. Appointment Of Data Processor.

a. The data manager shall only engage, appoint, use or involve a data processor to process personal data on its behalf through a valid contract.

b. The data processor referred to in sub-section (a) shall not further engage, appoint, use, or involve another data processor in the relevant processing on its behalf except with the authorization of the data manager, unless permitted through the contract referred to in sub-section (a).

c. The data processor, and any employee of the data manager or the data processor, shall only process personal data in accordance with the instructions of the data manager unless they are required to do otherwise under law and shall treat any personal data that comes within their knowledge as confidential.

43. Classification Of Data Managers As Significant Data Managers. —

a. The Authority shall, having regard to the following factors, notify certain data managers or classes of data managers as significant data managers—

i. quantity of personal data processed;
ii. sensitivity of personal data processed;
iii. turnover of the data manager;
iv. risk of harm resulting from any processing or any kind of processing undertaken by the manager;
v. use of new technologies for processing; and
vi. any other factor relevant in causing harm to any data subject as a consequence of such processing.

b. The notification of a data manager or classes of data managers as significant data managers by the Authority under sub-section (a) shall require such data manager or class of data managers to register with the Authority in such manner as may be specified.

c. All or any of the following obligations in this Chapter, as determined by the Authority, shall apply only to significant data managers—

i. data protection impact assessments under section 38;
ii. record-keeping under section 39;
iii. data audits under section 40; and
iv. data protection supervisor under section 41.

d. Notwithstanding sub-section (c), the Authority may notify the application of all or any of the obligations in sub-section (c) to such data manager or class of data managers, not being a significant data manager, if it is of the view that any processing activity undertaken by such data manager or class of data managers carries a risk of significant harm to data subjects.

44. Grievance Redressal. —

a. Every data manager shall have in place proper procedures and effective mechanisms to address grievances of data subjects efficiently and in a speedy manner.

b. A data subject may raise a grievance in case of a violation of any of the provisions of this Act, or rules prescribed, or regulations specified thereunder, which has caused or is likely to cause harm to such data subject, to—

   i. the data protection supervisor, in case of a significant data manager; or

   ii. an officer designated for this purpose, in case of any other data manager.

c. A grievance raised under sub-section (b) shall be resolved by the data manager in an expeditious manner and no later than thirty days from the date of receipt of grievance by such data manager.

d. Where, a grievance under sub-section (b) is not resolved within the time period mentioned under sub-section (c), or where the data subject is not satisfied with the manner in which the grievance is resolved, or the data manager has rejected the grievance raised, the data subject shall have the right to file a complaint with the adjudication wing under section 62 of the Act in the manner prescribed.

e. Any person aggrieved by an order made under this section by an Adjudicating Officer in accordance with the procedure prescribed in this regard, may prefer an appeal to the Appellate Tribunal.

45. Accountability.

a. The data manager shall be responsible for complying with all obligations set out in this Act in respect of any processing undertaken by it or on its behalf.

b. The data manager should be able to demonstrate that any processing undertaken by him or on his behalf is in accordance with the provisions of this Act.

Chapter VII The Data Protection Authority

46. Establishment

The Central Government shall, by notification, establish for the purposes of this Act, an Authority to be called the Data Protection Authority of India. The Authority shall be a body corporate, having perpetual succession and a common seal, with power, subject to the provisions of this Act, to acquire, hold and dispose of property, both movable and immovable, and to contract and shall, by the said name, sue or be sued.

47. Constitution

The Data Protection Authority shall consist of a Chairperson and six other full time serving Members, to exercise the jurisdiction and powers and discharge the functions and duties conferred or imposed upon it by or under this Act. The Chairperson and Members and other employees of the Data Protection Authority shall be deemed to be public servants within the meaning of **section** 21 of the Indian Penal Code, 1860 (45 of 1860).

i. Chairperson

The Chairperson shall be a person who has been a Judge of the Supreme Court or High Court: Provided that the appointment of

the Chairperson shall be made only after consultation with the Chief Justice of India and Cabinet Secretary.

ii. Members

Each Member shall be a person of ability, integrity and standing who has a special knowledge and professional experience of not less than ten years in field of data protection, information technology, data management, data science, data security, cyber and internet laws, and related subjects.

48. Terms Of Office

Terms of office conditions of service, etc. of Chairperson and Members are as below,

a. Before appointing any person as the Chairperson or Member, the Central Government shall satisfy itself that the person does not, and will not, have any such financial or other interest as is likely to affect prejudicially his functions as such Chairperson or Member.

b. The Chairperson and every Member shall hold office for period, not exceeding five years, as may be specified in the order of his appointment: Provided that no person shall hold office as the Chairperson or Member after he has attained the age of sixty-seven years.

c. Notwithstanding anything contained in sub-section (2), the Chairperson or any Member may –

   i. by writing under his hand resigns his office at any time

   ii. be removed from office in accordance with the provisions of section 49 of this Act.

d. A vacancy caused by the resignation or removal of the Chairperson or Member under subsection (c) shall be filled by fresh appointment within three months from the date of such vacancy.

i. In the event of the occurrence of a vacancy in the office of the Chairperson, such one of the Members as the Central Government may, by notification, authorise in his behalf, shall act as the Chairperson till the date on which a new Chairperson, appointed in accordance with the provisions of this Act, to fill such vacancy, enters upon his office.

ii. When the Chairperson is unable to discharge his functions owing to absence, illness or any other cause, such one of the Members as the Chairperson may authorise in writing in this behalf shall discharge the functions of the Chairperson, till the date on which the Chairperson resumes his duties.

e. The salaries and allowances payable to and the other terms and conditions of service of the Chairperson and Members shall be such as may be prescribed: Provided that neither the salary and allowances nor the other terms and conditions of service of the Chairperson and any member shall be varied to his disadvantage after his appointment.

49. Removal of Chairperson and Members from office

The Central Government may remove from office the Chairperson or any Member, who –

a. is adjudged an insolvent
b. engages during his term of office in any paid employment outside the duties of his office;
c. is unfit to continue in office by reason of infirmity of mind or body
d. is of unsound mind and stands so declared by a competent court
e. is convicted for an offence which in the opinion of the President involves moral turpitude
f. has acquired such financial or other interest as is likely to affect prejudicially his functions as a Chairperson or Member

g. has abused his position as to render his continuance in offence prejudicial to the public interest

50. Secretary, Officers, Other Employees Of The Data Protection Authority

a. The Central Government shall appoint a Secretary to the Data Protection Authority to exercise and perform, under the control of the Chairperson such powers and duties as may be prescribed or as may be specified by the Chairperson.

b. The Central Government may provide the Data Protection Authority with such other officers and employees as may be necessary for the efficient performance of the functions of the Data Protection Authority.

c. The salaries and allowances payable to and the conditions of service of the Secretary and other officers and employees of the Data Protection Authority shall be such as may be prescribed

51. Grants By Central Government.

The Central Government may, after due appropriation made by Parliament by law in this behalf, make to the Authority grants of such sums of money as it may think fit for the purposes of this Act.

52. Data Protection Funds.—

a. There shall be constituted a fund to be called the Data Protection Authority Fund to which the following shall be credited—

   i. all Government grants, fees and charges received by the Authority under this Act; and

   ii. all sums received by the Authority from such other source as may be decided upon by the Central Government, but which shall not include the sums mentioned in sub-section (c).

iii. The Data Protection Authority Fund shall be applied for meeting—

1. the salaries, allowances and other remuneration of the chairperson, members, officers, employees, consultants and experts appointed by the Authority; and
2. the other expenses of the Authority in connection with the discharge of its functions and for the purposes of this Act.

b. Without prejudice to the foregoing, there shall also be constituted a fund to be called the Data Protection Awareness Fund to which all sums realized by way of penalties by the Authority under this Act shall be credited.

53. Accounts and Audit

a. An annual statement account has to be prepared by the Authority while maintaining proper accounts and other relevant records. The annual statement of account has to be in accordance to the prescribed manner by the Central Government in consultation with the Comptroller and Auditor-General of India.

b. Auditing of the Authority's account shall be done by the Comptroller and Auditor-General of India at the prescribed intervals and if any expenditure incurred by Comptroller and Auditor-General while such auditing shall be reimbursed by the Authority.

c. The Comptroller and Auditor-General of India itself or any other person appointed by it to act on its behalf for auditing of the accounts of the Authority shall have the same rights, privileges and authority as generally has in connection with the audit of the Government accounts and, in particular, shall have the right to demand the production of

books, accounts, connected vouchers and other documents and papers, and to inspect any of the offices of the Authority.

d. The audit report of the accounts of the Authority shall be prepared by the Comptroller and Auditor-General of India or any other person acting on its behalf and thereon shall be forwarded to the Central Government and the Central Government shall cause the same to be laid before each House of the Parliament.

54. Furnishing of returns, etc. to Central Government.—

a. The Authority shall furnish to the Central Government at prescribed time, form and manner or as the Central Government may direct, such returns and statements and such particulars in regard to any proposed or existing programed for the promotion and development of protection of personal data, as the Central Government from time to time, require.

b. The Authority shall prepare once every year at prescribed time and form, an annual report giving a summary of its activities carried out in the previous year and copies of such report shall be forwarded to the Central Government.

c. A copy of the report received under sub-section (b) shall be laid, before each House of the Parliament.

55. Standard Functions Of The Authority

a. It shall be the foremost function of the Authority to safeguard the interests of data subjects, restrict any misuse of personal data, ensure compliance with the provisions of this Act, and endorse alertness of data protection.

b. Without prejudice to the generality of the foregoing and other functions set out under this Act, the functions of the Authority shall include—

i. supervising the safeguards provided by or under this Act and other law for the time being in force for the protection of data and recommend measures for their effective implementation;

ii. checking reasonable purposes for processing personal data as prescribed under section 9 (e) of this Act;

iii. taking an early and suitable action in response to a data security breach in accordance with the provisions of this Act;

iv. maintaining a database on its website containing names of significant data managers along with a rating in the form of a data trust score indicating compliance with the obligations of this Act by such managers;

v. specifying the criteria for assigning a rating in the form of a data trust score by a data auditor having regard to the factors mentioned in sub-section (2) of section 40;

vi. examination of any data audit reports submitted under section 40 of this Act and taking any action pursuant thereto in accordance with the provisions of this Act;

vii. issuance of a certificate of registration to data auditors and renewal, modification, withdrawal, suspension or cancellation thereof and maintaining a database on its website of such registered data auditors and specifying the requisite qualifications, code of conduct, practical training and functions to be performed by such data auditors;

viii. categorization and issuance of certificate of registration to significant data managers and renewal, modification, withdrawal, suspension or cancellation thereof under section 43**;**

ix. monitoring cross-border transfer of personal data under section 12 of this Act;

x. promoting awareness and knowledge of data protection amongst public through any means necessary;

xi. encouraging awareness among data managers of their obligations and duties under this Act;

xii. supervising technological developments and commercial practices from time to time that may affect protection of personal data;

xiii. undertaking and promoting research in the field of protection of data;

xiv. advising Parliament, Central Government, State Government and any regulatory or statutory authority on measures that must be undertaken to promote protection of personal data and ensuring consistency of application and enforcement of this Act;

xv. issuing guidance on any provision under this Act either on its own or in response to any query received from a data manager where the Authority considers it necessary, subject always to the provisions of this Act;

xvi. advising the Central Government on the acceptance of any relevant international instrument relating to protection of personal data;

xvii. specifying fees and other charges for carrying out the purposes of this Act;

xviii. inquiring Suo Moto or on a petition presented to it by any person, in respect of any matter connected with the collection, storage, processing, disclosure or other handling of any data and give such directions or pass such orders as are necessary for reasons to be recorded in writing.

xix. asking for information, directing inspections and inquiries into the activities of data managers in compliance with the provisions of this Act;

xx. publish periodic reports concerning the incidence of collection, processing, storage, disclosure and other handling of data;

xxi. executing such other tasks, comprising maintaining, updating and submitting of any records, documents, books, registers or any other data, as may be prescribed.

xxii. reviewing any measures taken by any entity for the protection of data and take such further action is it deems fit;

xxiii. reviewing any action, policy or procedure of any entity to ensure compliance with this Act and any rules made hereunder;

xxiv. formulating in consultation with experts, norms for the effective protection of data and suggesting the same to government;

xxv. encouraging the efforts of non-governmental organizations and institutions working in the field of data protection;

xxvi. such other functions as it may consider necessary for the protection of data.

(d) Where, the Authority processes personal data, it shall be taken as the data manager or the data processor in relation to such personal data as applicable, and where the Authority comes into possession of any information that is treated as confidential by the data manager or data processor, it shall not disclose such information unless required as per law, or where it is required to carry out its function under clause (xxii) of sub-section (b).

56. Office of Data Protection

Headquarter of the Data Protection Authority shall be at Delhi and the other offices of the Data Protection Authority shall be in the capital city of every state of India (for addressing the issues related to data protection at state level) while any other location must be directed by the Chairperson in consultation with the Central Government. The state branches would further maintain and

manage the adjudicating wings at district level to resolve the issues arising out of data protection breach at district level.

57. Power and authority

a. The Authority may, for the discharge of its functions under this Act, issue such directions from time to time as it may consider necessary to data manager or data processors generally, or to any data manager or data processor in particular, and such data manager or data processors, as the case may be, shall be bound to comply with such directions.

b. No such direction shall be issued under sub-section (a) unless the Authority has given a reasonable opportunity of being heard to the data manager or data processors concerned.

c. The Authority may, on a representation made to it or on its own motion, modify, suspend, withdraw or cancel any direction issued under sub-section (a) and in doing so, may impose such conditions as it thinks fit, subject to which the modification, suspension, withdrawal or cancellation shall have effect.

d. The Data Protection Authority shall, for the purposes of any inquiry or for any other purpose under this Act, have the same powers as vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying suits in respect of the following matters, namely –

   i. the summoning and enforcing the attendance of any person from any part of India and examining him on oath;
   ii. the discovery and production of any document or other material object producible as evidence;
   iii. the reception of evidence on affidavit;
   iv. the requisitioning of any public record from any court or office;
   v. the issuing of any commission for the examination of witnesses;
   vi. any other matter which may be prescribed;

e. The Data Protection Authority shall have power to require any person, subject to any privilege which may be claimed by that person under any law for the time being in force, to furnish information on such points or matters as, in the opinion of the Data Protection Authority, may be useful for, or relevant to, the subject matter of an inquiry and any person so required shall be deemed to be legally bound to furnish such information within the meaning of section 176 and section 177 of the Indian Penal Code, 1860 (45 of 1860).

f. The Data Protection Authority or any other officer, not below the rank of a Gazetted Officer, specially authorized in this behalf by the Data Protection Authority may enter any building or place where the Data Protection Authority has reason to believe that any document relating to the subject matter of the inquiry may be found, and may seize any such document or take extracts or copies therefrom subject to the provisions of section 100 of the Code of Criminal Procedure, 1973 (2 of 1974), in so far as it may be applicable.

g. The Data Protection Authority shall be deemed to be a civil court and when any offence as is described in section 175, section 178, section 179, section 180 or section 228 of the Indian Penal Code, 1860 (45 of 1860) is committed in the view or presence of the Data Protection Authority, the Data Protection Authority may, after recording the facts constituting the offence and the statement of the accused as provided for in the Code of Criminal Procedure, 1973 (2 of 1974), forward the case to a Magistrate having jurisdiction to try the same and the Magistrate to whom any such case is forwarded shall proceed to hear the complaint against the accused as if the case had been forwarded to him under **section** 346 of the Code of Criminal Procedure, 1973 (2 of 1974).

58. Meetings of the Authority.

a. The chairperson and members of the Authority shall meet at such times and places and shall observe such rules and procedures in regard to transaction of business at its meetings including quorum at such meetings, as may be prescribed.

b. If, for any reason, the chairperson is unable to attend any meeting of the Authority, any other member chosen by the members present at the meeting, shall preside at the meeting.

c. All questions which come up before any meeting of the Authority shall be decided by a majority of votes of the members present and voting, and in the event of an equality of votes, the chairperson or in her absence, the member presiding, shall have a casting or a second vote.

d. Any member who has any direct or indirect pecuniary interest in any matter coming up for consideration at a meeting of the Authority shall disclose the nature of her interest at such meeting, which shall be recorded in the proceedings of the Authority and such member shall not take part in any deliberation or decision of the Authority with respect to that matter.

59. Action To Be Taken By Authority Pursuant To An Inquiry.—

a. On receipt of a report under sub-section (d) of section 44, the Authority may, after giving such opportunity to the data manager or data processor to make a representation in connection with the report as the Authority deems reasonable, by an order in writing—

   i. warning the data manager or processor in writing for their activities which is likely to violate the provision of this Act;

   ii. warning data manager or processor in writing for their activities which has violated the provision of this Act;

iii. necessitating the data manager or processor to stop and discontinue such activities causing any violation of the provisions of this Act;

iv. mandates the data manager or processor to modify and carry activities which are in compliance to the provisions of this Act;

v. suspending or desisting activities of data manager or processor which is in infringing of the provisions of this Act for the time being;

vi. suspending or terminating registration of data manager or processor granted by the Adjudicating Officer;

vii. restricting any trans-border flow of personal data; or

viii. necessitate the data manager or processor to take any such action in respect of any matter arising out of the report as the Authority may think fit.

b. A data manager or processor aggrieved by an order made under this **section** by the Authority may prefer an appeal to the Appellate Tribunal.

60. Decisions And Ruling Of The Data Protection Authority

a. The decisions of the Data Protection Authority shall be binding.

b. In its decisions, the Data Protection Authority has the power to ,

i. require an entity to take such steps as may be necessary to secure compliance with the provisions of this Act;

ii. require an entity to compensate any person for any loss or detriment suffered;

c. Impose any of the penalties provided under this Act.

61. Vacancies Not An Excuse To Invalidate Proceedings Of The Authority.—

No act or proceeding of the Authority shall be invalid merely by reason of—

a. any vacancy or defect in the constitution of the Authority;

b. any defect in the appointment of a person as a chairperson or member; or,

c. any irregularity in the procedure of the Authority not affecting the merits of the case.

62. Appointment of Adjudicating Officer.

a. Without prejudice to any other provision of this Act and for the purpose of imposing of penalties under Chapter X or awarding compensation under section 98, the Authority shall have a separate adjudication wing.

b. The Central Government shall, having regard to the need to ensure the operational segregation, independence, and neutrality of the adjudication wing, prescribe—

i. number of Adjudicating Officers;

ii. qualification of Adjudicating Officers;

iii. manner and terms of appointment of Adjudicating Officers ensuring independence of such officers;

iv. jurisdiction of Adjudicating Officers;

v. procedure for carrying out an adjudication under this Act; and

vi. other such requirements as the Central Government may deem fit.

c. The Adjudicating Officers shall be persons of ability, integrity and standing, and must have specialized knowledge of, and not less than seven years professional experience in the fields of constitutional law, cyber and internet laws, information technology law and policy, data protection and related subjects.

63. General Duties Of Adjudicating Officer

a. **Enforcement Notice**

1. If the Adjudicating Officer is satisfied that a data manager has contravened or is contravening any of the data protection provisions, the Adjudicating Officer may serve him with a notice (in this Act referred to as "an enforcement notice") requiring him, for complying with the provisions in question, to do either or both of the following—
   i. to take within such time as may be specified in the notice, or to refrain from taking after such time as may be so specified, such steps as are so specified, or
   ii. to refrain from processing any personal data or any personal data of a description specified in the notice, or to refrain from processing them for a purpose so specified or in a manner so specified, after such time as may be so specified.
2. In deciding whether to serve an enforcement notice, the Adjudicating Officer considers whether the contravention has caused or is likely to cause any person damage or distress.
3. An enforcement notice may also require the data controller to rectify, block, erase or destroy any inaccurate data may also require the data controller to rectify, block, erase or destroy any other data held by him and containing an expression of opinion which appears to the Adjudicating Officer to be based on the inaccurate data.
4. The provisions of the notice are to be complied with before the end of the period of seven days beginning with the day on which the notice is served.
5. Notification regulations (as defined by section 25(b)) may make provision as the effect of the service of an enforcement notice on any entry in the register maintained under section 27 which relates to the person on whom the notice is served.

b. Request For Assessment

1. A request may be made to the Adjudicating Officer by or on behalf of any person who is, or believes himself to be, directly affected by any processing of personal data for an assessment as to whether it is likely or unlikely that the processing has been or is being carried out in compliance with the provisions of this Act.
2. On receiving a request under this section, the Adjudicating Officer shall make an assessment in such manner as appears to him to be appropriate, unless he has not been supplied with such information as he may reasonably require in order to—
   i. satisfy himself as to the identity of the person making the request, and
   ii. enable him to identify the processing in question.
3. The matters to which the Adjudicating Officer may have regard in determining in what manner it is appropriate to make an assessment include—
   i. the extent to which the request appears to him to raise a matter of substance,
   ii. any undue delay in making the request, and
   iii. whether or not the person making the request is entitled to make an application under section 18 in respect of the personal data in question.

c. Standard Duties

1. It shall be the duty of the Adjudicating Officer to promote the following of good practice by data manager and, in particular, so to perform his functions under this Act as to promote the observance of the requirements of this Act by data manager.
2. The Adjudicating Officer shall arrange for the dissemination in such form and manner as he considers appropriate of such information as it may appear to him expedient to give to the public about the operation of this Act, about good practice, and about other matters within the scope of his functions under this Act, and may give advice to any person as to any of those matters.

3. The Adjudicating Officer shall also—
   i. where he considers it appropriate to do so, encourage trade associations to prepare, and to disseminate to their members, such codes of practice, and
   ii. where any trade association submits a code of practice to him for his consideration, consider the code and, after such consultation with data subjects or persons representing data subjects as appears to him to be appropriate, notify the trade association whether in his opinion the code promotes the following of good practice.
4. The Adjudicating Officer may, with the consent of the data manager, assess any processing of personal data for the following of good practice and shall inform the data controller of the results of the assessment.
5. In this section—
   i. "good practice" means such practice in the processing of personal data as appears to the Adjudicating Officer to be desirable having regard to the interests of data subjects and others, and includes (but is not limited to) compliance with the requirements of this Act;
   ii. "trade association" includes any body representing data managers.

Explanation: Data Protection Authority shall be functioning as district level forum similar to that of consumer forum for grievance and redressal so that the aggrieved party may have cost effective justice. Moving to state tribunal every time would be more time consuming as well as very costly for the aggrieved party.

Chapter VIII Exemptions

64. National And State Security

a. Personal data are exempt from any of the provisions of this Act if data required is for the purpose of safeguarding national security.

b. Subject to subsection (d), a certificate signed by the President of India certifying that exemption from all or any of the provisions mentioned in the Act, is or at any time was required for the purpose there mentioned in respect of any personal data shall be conclusive evidence of that fact.

c. A certificate under subsection (b) may identify the personal data to which it applies by means of a general description and may be expressed to have prospective effect.

d. Any person directly affected by the issuing of a certificate under subsection (b) may appeal to the Tribunal against the certificate.

e. If on an appeal under subsection (d), the Tribunal finds that, applying the principles applied by the court on an application for judicial review, the President did not have reasonable grounds for issuing the certificate; the Tribunal may allow the appeal and quash the certificate.

f. Where in any proceedings under or by virtue of this Act it is claimed by a data manager that a certificate under subsection (b) which identifies the personal data to which it applies by means of a general description applies to any personal data, any other party to the proceedings may appeal to the Tribunal on the ground that the certificate does not apply to the personal data in question.

g. On any appeal under subsection (f), the Tribunal may determine that the certificate does not so apply.

h. A document purporting to be a certificate under subsection (b) shall be received in evidence and deemed to be such a certificate unless the contrary is proved.

i. A document which purports to be certified by or on behalf of a President as a true copy of a certificate issued by that Minister under subsection (b) shall in any legal proceedings be evidence (sufficient evidence) of that certificate.

j. The power conferred by subsection (b) on a President shall not be exercisable except by a Minister who is a member of the Cabinet.

65. Crime and Taxation

a. Personal data processed for any of the following purposes are exempt from the data protection provisions,

   i. the prevention or detection of crime,
   ii. the apprehension or prosecution of offenders, or
   iii. the assessment or collection of any tax or duty or of any imposition of a similar nature,

b. Personal data which are processed for the purpose of discharging statutory functions, and consist of information obtained for such a purpose from a person who had it in his possession for any of the purposes mentioned in subsection (a), are exempt from the subject information provisions to the same extent as personal data processed for any of the purposes mentioned in that subsection.

c. Personal data in respect of which the data manager is a relevant authority and which—

i. consist of a classification applied to the data subject as part of a system of risk assessment which is operated by that authority for either of the following purposes—

1. the assessment or collection of any tax or duty or any imposition of a similar nature, or
2. the prevention or detection of crime, or apprehension or prosecution of offenders, where the offence concerned involves any unlawful claim for any payment out of, or any unlawful application of, public funds.

ii. are processed for either of those purposes, are exempt from section 18 (Right to access) to the extent to which the exemption is required in the interests of the operation of the system.

c. In this subsection "public funds" includes funds provided by any Community institution; "relevant authority" means—

i. a government department,
ii. a local authority, or
iii. any other authority administering housing benefit or council tax benefit

66. Health, Education and Social Work

a. The Home Minister may by order exempt from the subject information provisions, or modify those provisions in relation to, personal data consisting of information as to the physical or mental health or condition of the data subject.

b. The Home Minister may by order exempt from the subject information provisions, or modify those provisions in relation to—

i. personal data in respect of which the data manager is the proprietor of, or a teacher at, a school, and which consist of

information relating to persons who are or have been pupils at the school, or

ii. personal data in respect of which the data manager is an education authority, and which consist of information relating to persons who are receiving, or have received, further education provided by the authority.

c. The Home Minister may by order exempt from the subject information provisions, or modify those provisions in relation to, personal data of such other descriptions as may be specified in the order, being information—

i. Processed by government departments or local authorities or by voluntary organisations or other bodies designated by or under the order, and

ii. appearing to him to be processed in the course of, or for the purposes of, carrying out social work in relation to the data subject or other individuals; but the Home Minister shall not under this subsection confer any exemption or make any modification except so far as he considers that the application to the data of those provisions (or of those provisions without modification) would be likely to prejudice the carrying out of social work.

d. In this section— "education authority" have the same meaning as in The Indian Education Act, 1835 and in relation to a school in means—

i. in the case of a self-governing school, the board of management within the meaning of the Self-Governing Schools etc.,

ii. in the case of an independent school, the proprietor of the school,

iii. in the case of a grant-aided school, the managers of the school, and

iv. in the case of a public school, the education authority

67. Regulatory Activity

a. Personal data processed for the purposes of discharging functions to which this subsection applies are exempt from the subject information provisions in any case to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of those functions.

b. Subsection (a) applies to any relevant function which is designed—

i. For protecting members of the public against—

1. financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate,
2. financial loss due to the conduct of discharged or undischarged bankrupts, or
3. dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity,

c. for protecting charities against misconduct or mismanagement (whether by trustees or other persons) in their administration,

d. for protecting the property of charities from loss or misapplication,

e. for the recovery of the property of charities,

f. for securing the health, safety and welfare of persons at work,

g. for protecting persons other than persons at work against risk to health or safety arising out of or in connection with the actions of persons at work.

h. In subsection (b) “relevant function” means—

i. any function conferred on any person by or under any enactment,

ii. any function of the Prime Minisiter, a Minister of the Cabinet or a government department, or

iii. any other function which is of a public nature and is exercised in the public interest.

i. Personal data processed for the purpose of discharging any function which is designed for protecting members of the public against—

i. mal-administration by public bodies,

ii. failures in services provided by public bodies, or

iii. a failure of a public body to provide a service which it was a function of the body to provide, are exempt from the subject information provisions in any case to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of that function.

j. Personal data processed for the purpose of discharging any function which is designed—

i. for protecting members of the public against conduct which may adversely affect their interests by persons carrying on a business,

ii. for regulating agreements or conduct which have as their object or effect the prevention, restriction or distortion of competition in connection with any commercial activity, or

iii. for regulating conduct on the part of one or more undertakings which amounts to the abuse of a dominant position in a market, are exempt from the subject information provisions in any case to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of that function.

68. Journalism, Literature and Art

a. Personal data which are processed only for the special purposes are exempt from any provision to which this subsection relates if—

   i. the processing is undertaken with a view to the publication by any person of any journalistic, literary or artistic material,

   ii. the data manager reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest, and

   iii. the data manager reasonably believes that, in all the circumstances, compliance with that provision is incompatible with the special purposes.

b. In considering for the purposes of subsection (a)(ii) whether the belief of a data manager that publication would be in the public interest was or is a reasonable one, regard may be had to his compliance with any code of practice which—

   i. is relevant to the publication in question, and

   ii. is designated by the Secretary of State by order for the purposes of this subsection.

c. Where at any time ("the relevant time") in any proceedings against a data manager under section 18 (Right to Access), or 19 (Rectification, Blocking, Erasure and Destruction), the data manager claims, or it appears to the court, that any personal data to which the proceedings relate are being processed—

   i. only for the special purposes, and

   ii. With a view to the publication by any person of any journalistic, literary or artistic material which, at the time

twenty-four hours immediately before the relevant time, had not previously been published by the data manager.

e. For the purposes of this Act "publish", in relation to journalistic, literary or artistic material, means make available to the public or any section of the public.

69. Research, History and Statistics

a. In this section "research purposes" includes statistical or historical purposes; "the relevant conditions", in relation to any processing of data, means the conditions—

   i. that the data are not processed to support measures or decisions with respect to particular individuals, and

   ii. that the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

b. The further processing of personal data only for research purposes in compliance with the relevant conditions is not to be regarded as incompatible with the purposes for which they were obtained.

c. Data especially personal data which are processed only for research purposes in compliance with the relevant conditions may be kept indefinitely.

d. Data which are processed only for research purposes are exempt from section 18 (Right to Access) if—

   i they are processed in compliance with the relevant conditions, and

   ii. the results of the research or any resulting statistics are not made available in a form which identifies data subjects or any of them.

e. For the purposes of subsections (b) to (d) data are not to be treated as processed otherwise than for research purposes merely because the data are disclosed—

i. to any person, for research purposes only,
ii. to the data subject or a person acting on his behalf,
iii. at the request, or with the consent, of the data subject or a person acting on his behalf, or
iv. in circumstances in which the person making the disclosure has reasonable grounds for believing that the disclosure falls within paragraph (i), (ii) or (iii).

70. Information Available To Public By Or Under Enact

Data are exempt from—

a. the subject information provisions,
b. the section 19(a) to (c) (Rectification, erasure, blocking and destruction),
c. the non-disclosure provisions

if the data consist of information which the data manager is obliged by or under any enactment to make available to the public, whether by publishing it, by making it available for inspection, or otherwise and whether gratuitously or on payment of a fee.

71. Disclosure Required By Law Or Made In Connection To Legal Proceedings

a. Personal data are exempt from the non-disclosure provisions where the disclosure is required by or under any enactment, by any rule of law or by the order of a court.
b. Personal data are exempt from the non-disclosure provisions where the disclosure is necessary—

i. for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), or
ii. for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

72. Domestic Purposes

Personal data processed by an individual only for the purposes of that individual's personal, family or household affairs (including recreational purposes) are exempt from the data protection provisions.

73. Anonymised Data

Data are anonymised if all identifying elements have been eliminated from a set of personal data. No element may remain in the information which could, by exercising reasonable effort, serve to re-identify the person(s) concerned. Where data have been successfully anonymised, they are no longer personal data. If personal data no longer serve their initial purpose, but are to be kept in a personalized form for the purpose of historical, statistical or scientific use, then such data is exempted from The Data Protection Act.

74. Powers to make further exemptions by order

a. The President may by order exempt from the subject information provisions data consisting of information the disclosure of which is prohibited or restricted by or under any enactment if and to the extent that he considers it necessary for the safeguarding of the interests of the data subject or the rights and freedoms of any other individual that the prohibition or restriction ought to prevail over those provisions.
b. The President may by order exempt from the nondisclosure provisions any disclosures of data made in circumstances specified in the order, if

he considers the exemption is necessary for the safeguarding of the interests of the data subject or the rights and freedoms of any other individual.

CHAPTER IX APPELLATE TRIBUNAL

75. Establishment of Appellate Tribunal.—

a. The Central Government shall, by notification, establish an Appellate Tribunal to—

   i. hear and dispose of any appeal from an order of the Adjudicating Officer under sub-section (e) of section 44;

   ii. hear and dispose of any appeal from an order of the Adjudicating Officer under sub-section (e) of section 97**; and**

   iii**.** hear and dispose of any appeal from an order of an Adjudicating Officer under sub-section (g) of section 98.

b. The Appellate Tribunal shall consist of a chairperson and such number of members as may be notified by the Central Government.

c. The Appellate Tribunal shall be set up at every capital city of the state to address the data protection breach issues at the state level.

d. Where, in the opinion of the Central Government, any existing body is competent to discharge the functions of the Appellate Tribunal as envisaged under this Act, and then the Central Government may notify such existing body to act as the Appellate Tribunal under this Act.

e. A National Appellate Tribunal shall be established (similar to that of national forum under Consumer Protection Act) by the Central Government by notification for handling the appeal done by the either party who are not satisfied with the decision of the State Appellate Tribunal.

76. Qualifications, Appointment, Term, Conditions Of Service Of Members.—

a. The Central Government may prescribe the qualifications, appointment, term of office, salaries and allowances, resignation, removal and the other terms and conditions of service of the chairperson and any member of the Appellate Tribunal.

b. Neither the salary and allowances nor the other terms and conditions of service of the chairperson or member of the Appellate Tribunal may be varied to her disadvantage after her appointment.

77. Vacancies.—

If, for reason other than temporary absence, any vacancy occurs in the office of the chairperson or a member of the Appellate Tribunal, the Central Government shall appoint another person in accordance with the provisions of this Act and the rules prescribed to fill the vacancy and the proceedings may be continued before the Appellate Tribunal from the stage at which the vacancy is filled.

78. Staff Of Appellate Tribunal.—

a. The Central Government shall provide the Appellate Tribunal with such officers and employees as it may deem fit.

b. The officers and employees of the Appellate Tribunal shall discharge their functions under the general superintendence of its chairperson.

c. The salaries and allowances and other conditions of service of such officers and employees of the Appellate Tribunal shall be such as may be prescribed.

79. Distribution Of Business Amongst Benches.—

a. Subject to the provisions of this Act, the jurisdiction of the Appellate Tribunal may be exercised by benches thereof, which shall be constituted by the chairperson.

b. Where benches of the Appellate Tribunal are constituted under sub-section (a), the chairperson may, from time to time, by notification, make provisions as to the distribution of the business of the Appellate Tribunal amongst the benches, transfer of members between benches, and also provide for the matters which may be dealt with by each bench.

c. On the application of any of the parties and after notice to the parties, and after hearing such of them as the chairperson may desire to be heard, or on the chairperson's own motion without such notice, the chairperson of the Appellate Tribunal may transfer any case pending before one bench, for disposal, to any other bench.

80. Appeals To Appellate Tribunal.—

a. Any person may file an appeal or application, as the case may be, with the Appellate Tribunal in such form, verified in such manner and is accompanied by such fee, as may be prescribed.

b. Any appeal or application to the Appellate Tribunal, as the case may be shall be preferred within a period of thirty days from the date on which a copy of the decision or order made by the Authority or the Adjudicating Officer, as the case may be, is received by the appellant or applicant and it shall be in such form, verified in such manner and be accompanied by such fee as may be prescribed.

c. Notwithstanding sub-section (b), the Appellate Tribunal may entertain any appeal or application, as the case may be, after the expiry of the said period of thirty days if it is satisfied that there was sufficient cause for not filing it within that period.

d. On receipt of an appeal or application, as the case may be, under this section, the Appellate Tribunal may, after providing the parties to the dispute or appeal, an opportunity of being heard, pass such orders thereon as it thinks fit.

e. The Appellate Tribunal shall send a copy of every order made by it to the parties to the dispute or the appeal and to the Authority, as the case may be.

f. The Appellate Tribunal may, for the purpose of examining the legality or propriety or correctness, of any decision, or order of the Authority or Adjudicating Officer referred to in the appeal or application preferred under this section, on its own motion or otherwise, call for the records relevant to disposing of such appeal or application and make such orders as it thinks fit.

81. Procedure And Powers Of Appellate Tribunal.—

a. The Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908), but shall be guided by the principles of natural justice and, subject to the other provisions of this Act, the Appellate Tribunal shall have powers to regulate its own procedure.

b. The Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely—

   i. summoning and enforcing the attendance of any person and examining her on oath;

   ii. requiring the discovery and production of documents;

   iii. receiving evidence on affidavits;

iv. subject to the provisions of section 123 and section 124 of the Indian Evidence Act, 1872 (1 of 1872), requisitioning any public record or document or a copy of such record or document, from any office;

v. issuing commissions for the examination of witnesses or documents;

vi. reviewing its decisions;

vii. dismissing an application for default or deciding it, *ex parte*;

viii. setting aside any order of dismissal of any application for default or any order passed by it, *ex parte*; and

ix. any other matter which may be prescribed.

c. Every proceeding before the Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code, 1860 (45 of 1860) and the Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973 (2 of 1974).

82. Orders Passed By Appellate Tribunal To Be Executable As A Decree.

a. An order passed by the Appellate Tribunal under this Act shall be executable by the Appellate Tribunal as a decree of civil court, and for this purpose, the Appellate Tribunal shall have all the powers of a civil court.

b. Notwithstanding anything contained in sub-section (a), the Appellate Tribunal may transmit any order made by it to a civil court having local jurisdiction and such civil court shall execute the order as if it were a decree made by that court.

c. The order passed by the State Appellate Tribunal shall be challenged at the National Appellate Tribunal within 30 days from the date the order passed by the State Appellate Tribunal.

83. Appeal To Supreme Court Of India.—

a. Notwithstanding anything contained in the Code of Civil Procedure, 1908 (5 of 1908) or in any other law, an appeal shall lie against any order of the Appellate Tribunal to the Supreme Court of India.
b. No appeal shall lie against any decision or order made by the Appellate Tribunal with the consent of the parties.
c. Every appeal under this section shall be preferred within a period of ninety days from the date of the decision or order appealed against.
d. Notwithstanding sub-section (c), the Supreme Court of India may entertain the appeal after the expiry of the said period of ninety days, if it is satisfied that the appellant was prevented by sufficient cause from preferring the appeal in time.

84. Right To Legal Representation.

The applicant or appellant may either appear in person or authorize one or more legal practitioners or any of its officers (which means an advocate, or an attorney and includes a pleader in practice) to present her or its case before the Appellate Tribunal.

85. Civil Court Not To Have Jurisdiction.—

No civil court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which the Appellate Tribunal is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

Explanation: The constitution of the State Appellate Tribunal shall be same at the National Appellate Tribunal. Moreover, at the national level the chairperson must be retired judge of Supreme Court and must be appointed with the consultation of the chief justice of India, while at the state level the chairperson must be retired judge of high court and must be a person nominated by the chief justice of the state high court.

Chapter X OFFENCES AND PENALTIES

86. Punishment For Offences Related To Personal Data

a. Whoever, except in conformity with the provisions of this Act, collects, receives, stores, processes, transfers, sell or offer to sell or otherwise handles any personal data and thereby causing harm to the data subject shall be punishable with imprisonment for a term which may extend to five years and may also be liable to fine which may extend to three lakh rupees or both.

b. Whoever even merely attempts to commit any offence under sub section (a) shall be punishable with the punishment provided for such offence under that sub-section.

c. Whoever, except in conformity with the provisions of this Act, collects, receives, stores, processes, transfers, sell or offer to sell or otherwise handles any sensitive personal data and thereby causing any harm to the data subject shall be punishable with imprisonment for a term which may extend to seven years and may also be liable to fine which may extend to five lakh rupees or both.

d. Whoever even merely attempts to commit any offence under sub section (c) shall be punishable with the punishment provided for such offence under that sub-section.

87. Re-Identification And Processing Of Anonymised Personal Data. —

a. Any person who, knowingly or intentionally or recklessly—

   i. re-identifies personal data which has been anonymized by a data manager or a data processor, as the case may be; or

   ii. re-identifies and processes such personal data as mentioned in clause (i) without the consent of such data manager or data processor, then such person shall be punishable with imprisonment for a term not exceeding five years or shall be liable to a fine which may extend up to rupees three lakh or both.

b. Nothing contained in sub-section (a) shall render any such person liable to any punishment provided under this section, if the person proves that—

   i. the personal data belongs to the person charged with the offence under sub-section (a); or

   ii. the data subject whose personal data is in question has explicitly consented to such re-identification or processing as per the provisions of this Act.

88. Abetment And Repeat Offenders

a. Whoever abets any offence punishable under this Act shall, if the act abetted is committed in consequence of the abetment, be punishable with the punishment provided for that offence.

b. Whoever, having been convicted of an offence under any provision of this Act is again convicted of an offence under the same provision, shall be punishable, for the second and for each subsequent offence, with double the penalty provided for that offence.

89. Offences and Penalty For Data Managers.

a. Where the data manager contravenes any of the following provisions, he shall be liable to a penalty which may extend up to seven crore rupees or the amount decided after analyzing the monetary gain he has made by committing such act by the appropriate tribunal or court, whichever is higher, as applicable—

   i. duty to take prompt and appropriate action in response to a data security breach under section 37 of this Act;

   ii. duty to undertake a data protection impact assessment by a significant data manager under section 38 of this Act;

   iii. duty to conduct a data audit by a significant data manager under section 40 of this Act;

   iv. appointment of a data protection supervisor by a significant data manager under section 41 of this Act;

   v. fails to register with the Authority under sub-section (b) of section 43**.**

b. Where a data manager contravenes any of the following provisions, it shall be liable to a penalty which may extend up to fifteen crore rupees or the amount decided after analyzing the monetary gain he has made by committing such act by the appropriate tribunal or court,, whichever is higher, as applicable—

   i. processing of personal data in violation of the provisions of Chapter II;

   ii. processing of personal data in violation of the provisions of section 9;

   iii. processing of sensitive personal data in violation of the provisions of section 16 of this Act;

   iv. processing of personal data of children in violation of the provisions of Chapter III;

v. failure to adhere to security safeguards as per section 36 of this Act;

vi. transfer of personal data outside India in violation of section 12 of this Act.

vii. the coalition of the overall economic interests of the data manager and the group entity;

viii. the rapport of the data manager and the group entity specifically with reference to the processing activity undertaken by the data manager; and

ix. the degree of control exercised by the group entity over the data manager or vice versa, as the case may be.

90. Penalty For Failure To Comply With Data Subject's Requests Under Chapter IV.—

Where, any data manager, without any reasonable clarification, fails to comply with any request made by a data subject under Chapter IV of this Act, such data manager shall be liable to a penalty of ten thousand rupees for each day during which such default continues, subject to a maximum of ten lakh rupees in case of significant data manager and five lakh rupees in other cases.

91. Penalty For Failure To Furnish Report, Returns, Information, Etc.—

If any data manager, who is required under this Act, or rules prescribed or regulations specified thereunder, to furnish any report, return or information to the Authority, fails to furnish the same, then such data manager shall be liable to penalty which shall be fifteen thousand rupees for each day during which such default continues, subject to a maximum of twenty lakh rupees in case of significant data managers and five lakh rupees in other cases.

92. Penalty For Failure To Comply With Direction Or Order Issued By The Authority.—

If any data manager or data processor fails to comply with any direction issued by the Authority under section 57 or order issued by the Authority under section 59, as applicable, such data manager or data processor shall be liable to a penalty which, in case of a data manager may extend to twenty thousand rupees for each day during which such default continues, subject to a maximum of two crore rupees, and in case of a data processor may extend to five thousand rupees for each day during which such default continues, subject to a maximum of fifty lakh rupees.

93. Offences And Penalty For Companies

a. Where an offence under this Act has been committed by a company, every person who, at the time of the offence was committed, was in charge of, and was responsible to, the company for the conduct of the business of the company, as well as the company shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly:

   Provided that nothing contained in this sub-section shall render any such person liable to any punishment, if he proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence.

b. Notwithstanding anything contained in sub-section (a), where any offence under this Act has been committed by a company and it is proved that the offence has been committed with the consent or connivance of, or is attributable to any neglect on the part of any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall be deemed to be guilty

of that offence, and shall be liable to be proceeded against and punished accordingly.

94. Offences To Be Cognizable And Non-Bailable.

Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), an offence punishable under this Act shall be cognizable and non-bailable.

95. Offences By Central Or State Government Departments.

a. The head of the department or authority shall be considered to be guilty of the offence committed by any of the department of the Central or State Government, or any authority of the State, and shall be liable to be proceeded against and punished accordingly:

   Provided that nothing contained in this sub-section shall render any such person liable to any punishment, if he proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence.

b. Notwithstanding anything contained in sub-section (a), where an offence under this Act has been committed by a department of the Central or State Government, or any authority of the State and it is proved that the offence has been committed with the consent or connivance of, or is attributable to any neglect on the part of, any officer, other than the head of the department or authority, such officer shall also be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

96. General Penalty

Whoever, in any case in which a penalty is not expressly provided by this Act, fails to comply with any notice or order issued under any provisions thereof, or

otherwise contravenes any of the provisions of this Act, shall be punishable with fine which may extend to one crore rupees, and, in the case of a continuing failure or contravention, with an additional fine which may extend to twelve thousand rupees for every day during which he has persisted in such failure or contravention.

97. Adjudication By Adjudicating Officer.—

a. No penalty shall be imposed under this Chapter except after conducting an inquiry in such manner as may be prescribed, and the data manager or data processor or any person, as the case may be, has been given a reasonable opportunity of being heard.

b. While holding an inquiry, the Adjudicating Officer shall have the power to summon and enforce the attendance of any person acquainted with the facts and circumstances of the case to give evidence or to produce any document which, in the opinion of the Adjudicating Officer, may be useful for or relevant to the subject matter of the inquiry.

c. If, on the conclusion of such inquiry, the Adjudicating Officer is satisfied that the person has failed to comply with the provisions of this Act or has caused harm to any data subject as a result of any violation of the provisions of this Act, which a penalty may be imposed under Chapter X, the Adjudicating Officer may impose a penalty in accordance with the provisions of the appropriate section.

d. While deciding whether to impose a penalty under sub-section (c) of this section and in determining the quantum of penalty under Chapter X, the Adjudicating Officer shall have due regard to the following factors, as may be applicable —

    i. nature, gravity and duration of violation taking into account the nature, scope and purpose of processing concerned;

ii. number of data subjects affected, and the level of harm suffered by them;

iii. intentional or negligent character of the violation;

iv. nature of personal data impacted by the violation;

v. repetitive nature of the default;

vi. transparency and accountability measures implemented by the data manager or data processor including adherence to any relevant code of practice relating to security safeguards;

vii. action taken by the data manager or data processor to mitigate the harm suffered by data subjects; and

viii. any other aggravating or mitigating factors relevant to the circumstances of the case, such as, the amount of disproportionate gain or unfair advantage, wherever quantifiable, made as a result of the default.

e. Any person aggrieved by an order under this section by the Adjudicating Officer may prefer an appeal to the Appellate Tribunal.

98. Compensation.

a. Any data subject who has suffered harm as a result of any violation of any provision under this Act, by a data manager or a data processor, shall have the right to seek compensation from the data manager or the data processor, as the case may be:

Provided data processor must be treated with reference to the work to him by data manager. When the data processor has acted beyond or contrary to the directions of the data manager, or is found to have executed his duties in a negligent way, or when the data processor has not exercised appropriate safeguards, or when the data processor has violated provisions laid down under the Act, then he shall be liable for the above laid conditions.

b. The data subject may seek compensation under this section pursuant to a complaint instituted in such form and manner as may be prescribed before an Adjudicating Officer.

c. Where there are one or more data subjects or any identifiable class of data subjects who have suffered harm as a result of any violation by the same data manager or data processor, one complaint may be instituted on behalf of all such subjects seeking compensation for the harm suffered.

d. While deciding whether to award compensation and the amount of compensation under this section, the Adjudicating Officer shall have due regard to the following factors, namely—

   i. nature, duration and extent of violation of the provisions of the Act, rules prescribed, or regulations specified there under;

   ii. nature and extent of harm suffered to the data subject;

   iii. intentional or negligent character of the violation;

   iv. supervising the proper execution of the duties of data manager or the data processor;

   v. action taken by the data manager or the data processor, as the case may be, to mitigate the damage suffered by the data subject;

   vi. checking for repetitive violation by the data manager or the data processor, as the case may be;

   vii. whether the arrangement between the data manager and data processor contains measures to safeguard the personal data being processed by the data processor on behalf of the data manager;

   viii. any other aggravating or mitigating factor relevant to the circumstances of the case, such as, the amount of disproportionate gain or unfair advantage, wherever quantifiable, made as a result of the default.

e. Where more than one data manager or data processor, or both a data manager and a data processor are involved in the same processing activity and are found to have caused harm to the data subject as per this section, then each data manager or data processor may be ordered to pay the entire compensation for the harm in order to ensure effective and speedy compensation to the data subject.

f. Where a data manager or a data processor has, in accordance with sub-section (e), paid the entire amount of compensation for the harm suffered by the data subject, such data manager or data processor shall be entitled to claim from the other data managers or data processors, as the case may be, that amount of compensation corresponding to their part of responsibility for the harm caused.

g. Any person aggrieved by an order made under this section by the Adjudicating Officer may prefer an appeal to the Appellate Tribunal.

99. Punishment Or Compensation To Be Without Prejudice To Any Other Action

The award or punishment for an offence under this Act shall be without prejudice to any other action which has been or which may be taken under any other law for the time being in force with respect to such contravention.

100. Recovery Of Amounts.—

a. The Authority shall, by an order in writing, appoint at least one officer or employee as a Recovery Officer for the purpose of this Act.

b. Where any person fails to comply with—

   i. an order of the Adjudicating Officer imposing a penalty under the provisions of this Act; or

ii. an order of the Adjudicating Officer directing payment of compensation under the provisions of this Act,

the Recovery Officer may recover from such person the aforesaid amount in any of the following ways, in descending order of priority, namely—

(i) attachment and sale of the person's movable property;

(ii) attachment of the person's bank accounts;

(iii) attachment and sale of the person's immovable property;

(iv) arrest and detention of the person in prison;

(v) appointing a receiver for the management of the person's movable and immovable properties.

c. For the purpose of such recovery, the provisions of section 220 to section 227, and sections 228A, 229 and 232, the Second and Third Schedules of the Income Tax Act, 1961 (43 of 1961) and the Income Tax (Certificate Proceedings) Rules, 1962, as in force from time to time, in so far as may be, shall apply with necessary modifications as if the said provisions and rules—

i. were the provisions of this Act; and

ii. referred to the amount due under this Act instead of to income tax under the Income Tax Act, 1961 (43 of 1961).

d. In this section, the movable or immovable property or monies held in a bank account shall include property or monies which meet all the following conditions—

i. property or monies transferred by the person without adequate consideration;

ii. such transfer is made:

1. on or after the date on which the amount in the certificate drawn up under section 222 of the Income Tax Act, 1961 (43 of 1961) had become due; and

2. to the person's spouse, minor child, son's wife or son's minor child.

iii.such property or monies are held by, or stand in the name of, any of the persons referred to in sub-clause (ii), including where they are so held or stand in the name of such persons after they have attained the age of majority.

e. The Recovery Officer shall be empowered to seek the assistance of the local district administration while exercising the powers under this section.

CHAPTER XI Miscellaneous Provisions

101. Power Of Central Government To Issue Directions In Certain Circumstances. —

a. The Central Government may, from time to time, issue to the Authority such directions as it may think necessary in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order.

b. Without prejudice to the foregoing provisions of this Act, the Authority shall, in exercise of its powers or the performance of its functions under this Act, be bound by such directions on questions of policy as the Central Government may give in writing to it from time to time:

c. Any direction issued by the Central Government shall, as far as practicable, be given, after providing an opportunity to the Authority to express its views in this regard.

d. The decision of the Central Government on whether a question is one of policy or not, shall be final.

102. Members, Etc., To Be Public Servants. —

The chairperson, members, officers and employees of the Authority and the Appellate Tribunal shall be deemed, when acting or purporting to act in

pursuance of any of the provisions of this Act, to be public servants within the meaning of section 21 of the Indian Penal Code, 1860 (45 of 1860).

103. Protection Of Action Taken In Good Faith. —

No suit, prosecution or other legal proceedings shall lie against the Authority or its chairperson, member, employee or officer for anything which is done in good faith or intended to be done under this Act, or the rules prescribed, or the regulations specified thereunder.

104. Exemption From Tax On Income. —

Notwithstanding anything contained in the Income Tax Act, 1961 (43 of 1961) or any other enactment for the time being in force relating to tax on income, profits or gains, as the case may be, the Authority shall not be liable to pay income tax or any other tax in respect of its income, profits or gains derived.

105. Delegation.

The chairperson of the Authority may, by general or special order in writing delegate to any member or officer of the Authority subject to such conditions, if any, as may be specified in the order, such of its powers and functions under this Act except the powers under section 111 as it may deem necessary.

106. Power To Remove Difficulties.

a. If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order, published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as may appear to be necessary or expedient for removing the difficulty.

b. No such order shall be made under this section after the expiry of five years from the commencement of this Act.

c. Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

107. Power To Exempt Certain Data Processors.

The Central Government may, by notification, exempt from the application of this Act or any provisions of this Act, processing of personal data of data subjects not within the territory of India, pursuant to any contract entered into with any person outside the territory of India, including any company incorporated outside the territory of India, by any data processor or any class of data processors incorporated under Indian law.

108. No Application To Non-Personal Data

Nothing contained in this Act shall affect the power of the Central Government to formulate appropriate policies for the digital economy, including measures for its growth, security, integrity, prevention of misuse, insofar as such policies do not govern personal data.

109. Bar On Processing Certain Forms Of Biometric Data

No data manager shall process such biometric data as may be notified by the Central Government, unless such processing is permitted by law.

110. Power To Make Rules. —

a. The Central Government may, by notification, make rules to carry out the purposes of this Act.

b. In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely—

    1. the manner in which a complaint with the adjudication wing may be filed under sub-section (d) of section 44;

2. the countries, sectors within a country, or international organisations to which transfers may be permitted under section 12;
3. the time period of notification to the Authority under section 12 of the transfer of personal data to a particular country;
4. the place of establishment and incorporation of the head office of the Authority as under section 56;
5. procedure to be followed by the selection committee under section 62;
6. the salaries and allowances payable to, and other terms and conditions of service of the chairperson and the members of the Authority under Chapter VII;
7. the times and places for, and the rules and procedures in regard to, transaction of business at the meetings of the Authority under sub-section (a) of section 58;
8. the time in which, and the form and manner in which the returns, statements, and particulars are to be furnished to the Central Government under sub-section (a) of section 54;
9. the time in which, and the form in which an annual report is to be prepared by the Authority and forwarded to the Central Government under sub-section (b) of section 54;
10. other functions of the Authority under clause (x) of sub-section (b) of section 55;
11. other matters under section 55 in respect of which the Authority shall have powers under the Code of Civil Procedure, 1908 (5 of 1908) that are vested in a civil court while trying a suit;
12. the number of Adjudicating Officers that the adjudication wing will consist of under sub-section (b) of section 62;

13. the qualification, manner and terms of appointment, and jurisdiction of Adjudicating Officers to ensure their independence, and the procedure for carrying out adjudication under this Act and other such requirements as deemed fit by the Central Government under sub-section (b) of section 62**;**
14. the manner in which the Adjudicating Officer will conduct an inquiry under sub-section (a) of section 97;
15. the form and manner of instituting a complaint under sub-section (b) of section 98;
16. the procedure for hearing of a complaint and the limit on the amount of compensation under sub-section (8) of section 75;
17. the qualifications, appointment, term of office, salaries and allowances, resignation, removal and the other terms and conditions of service of the chairperson and any member of the Appellate Tribunal under sub-section (b) of section 76;
18. the procedure of filling of vacancies in the Appellate Tribunal under section 77;
19. the salaries and allowances and other conditions of service of the officers and employees of the Appellate Tribunal under sub-section (c) of section 78;
20. the form, manner and fee for filing an appeal or application, as the case may be, with the Appellate Tribunal under sub-section (a) of section 80; and
21. other matters under clause (i) of sub-section (b) of section 81 in respect of which the Appellate Tribunal shall have powers under the Code of Civil Procedure, 1908 (5 of 1908) that are vested in a civil court while trying a suit.

111. Power To Make Regulations.

a. The Authority may, by notification, make regulations consistent with this Act and the rules prescribed there under to carry out the purposes of this Act.

b. In particular and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely:

1. information required to be provided by the data manager to the data subject in its notice under clause (xiv) of sub-section (a) of section 10;
2. manner in which the personal data retained by the data manager must be deleted under section 8;
3. reasonable purposes for which personal data may be processed in accordance with sub-section (e) of section 9;
4. safeguards as may be appropriate for protecting the rights of data subjects under sub-section (c) of section 9;
5. the additional factors necessary for determining the appropriateness of age verification mechanisms to be incorporated by a data manager processing the personal data and sensitive personal data of children under sub-section (c) of section 17;
6. practices that may be undertaken by data managers offering counseling or child protection services under sub-section (f) of section 17;
7. the time period within which a data manager must comply with a request made under sub-section (c) of section 24;
8. the time period within which a data subject may file a complaint under sub-section (d) of section 24;

9. the form in which the data manager is required to make available to the data subject information under sub-section (a) of section 35;
10. the manner by which a data manager shall notify the data subject regarding important operations in the processing of personal data under sub-section (b) of section 35;
11. the manner of periodic review of security safeguards to be undertaken by the data manager and the data processor under sub-section (b) of section 36;
12. the circumstances or classes of data managers or processing operations where it is mandatory to carry out data protection impact assessments under sub-section (b) of section 38;
13. the instances where a data auditor under this Act shall be engaged by the data manager to undertake a data protection impact assessment under sub-section (b) of section 38;
14. the manner in which the data manager shall submit the data protection impact assessment to the Authority under sub-section (d) of section 38;
15. any aspect of processing for which records shall be maintained under clause (iv) of sub-section (a) of section 39;
16. the form in which records shall be maintained under sub-section (b) of section 39;
17. the factors to be taken into consideration while evaluating the compliance of data managers with the provisions of this Act under sub-section (b) of section 40;
18. the form, manner and procedure by which data audits shall be conducted under sub-section (c) of section 40;

19. criteria on the basis of which rating in the form of a data trust score may be assigned to a data manager under sub-section (f) of section 40;
20. the eligibility, qualifications and functions to be performed by data auditors under sub-section (d) of section 40;
21. the eligibility and qualification of a data protection officer under sub-section (c) of section 41;
22. the registration requirements of significant data managers under sub-section (b) of section 43;
23. the provisions of the Act which may be exempted for different categories of research, archival or statistical purposes under section 69;
24. any other matter which is required to be, or may be specified, or in respect of which provision is to be or may be made by regulations.

112. Rules And Regulations To Be Laid Before Parliament.

Every rule and regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or regulation or, both Houses agree that the rule or regulation should not be made, the rule or regulation shall thereafter have effect only in such modified form or be of no effect, as the case may be; however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule or regulation.

113. Overriding Effect Of This Act.

Save as otherwise expressly provided under this Act, the provisions of this Act shall have an overriding effect to the extent that such provisions are inconsistent with any other law for the time being in force or any instrument having effect by virtue of any such law.

Notification : The Draft Bill is inspired from the Data Protection Directives, the Personal Data Protection Bill, 2006, the Approach paper for a legislation on privacy, published by Government of India, Ministry of Personnel, PG & Pensions Department of Personnel Training on 25th October 2010, Right to Privacy Bill, 2011, Report of the Group of Experts on Privacy (Chaired by Justice A P Shah, Former Chief Justice, Delhi High Court), 2012 and lastly The Personal Data Protection Bill, 2018 open for discussion by Justice B. N. Shrikrishna.

BIBLIOGRAPHY

1. Articles Referred :

1. Policy-Making, Technology And Privacy In India by subhajit basu.
2. Historical Analysis on European Data Protection Regulations. by Petra Hoepner, Linda Strick, Martin Löhe.
3. Data Protection Law In USA, by Robert Hasty, Dr. Trevor W. Nagel and Mariam Subjally, available at https://www.neighborhoodindicators.org/sites/default/files/course materials/A4ID_DataProtectionLaw%20.pdf
4. Data Safety and Privacy Protection, by Venkararmana B. Ramanathan, available at http://www.legalserviceindia.com/articles/Data_Safety.htm.
5. Data Protection, by R K Dewan available at http://www.rkdewan.com/dataprotection.php.
6. European Innovation Partnership, published by European Commission, available at https://ec.europa.eu/eip/ageing/standards/ict-and-communication/data/directive-9546ec_en.
7. Data Protection Law In India-Needs And Position by Adv. Swati Sinha.
8. New Challenges To Data Protection: Final Report. By European Commission
9. Data Protection Law in India. by Shojan Jacob.
10. Web 20 (Social Media) Policies in Higher Education, by Anne Arendt, Utah Valley University available at https://www.slideshare.net/annearendt/web-20-social-media-policies-in-higher-education.
11. What are the laws - Data Protection, Data Transmission and Export and Data Encryption in India to operate a technology platform for data processing? Answer by Prakash Prasad available on https://www.quora.com/What-are-the-laws-Data-Protection-Data-Transmission-and-Export-and-Data-Encryption-in-India-to-operate-a-technology-platform-for-data-processing
12. India's New Data Protection Legislation, by Raghunath Ananthapur, published in journal named Scripted available at https://script-

ed.org/article/indias-data-protection-legislation/

13. Data Protection In India, article by Majmudar & Co. available at https://www.scribd.com/document/136287003/Data-Protection-in-India
14. Freedom of Speech, The EU Data Protection Directive and the Swedish Personal Data Act. available at www.dsv.su.se/jpalme/society/eu-data-directive-freedom.html.
15. Attitudes Towards Privacy: A Comparison of India and the United States, by Jane Hils Shea, available at https://www.frostbrowntodd.com/resources-214.html.
16. Data Protection Law In India by Pankaj Kumar - Student of 4th year student, Bangalore Institute of Legal Studies, Bangalore available at http://www.legalserviceindia.com/article/l37-Data-Protection-Law-in-India.html
17. Right To Privacy Bill 2010 – A Few Comments, by Elonnai Hickok, available at https://cis-india.org/internet-governance/blog/privacy/privacy-bill-2010
18. Report of the Group of Experts on Privacy (Chaired by Justice A P Shah, Former Chief Justice, Delhi High Court) by Government of India
19. Data Protection In India : by Majumdar & Co.
20. Data Protection Overview. by Tapan Ray
21. Article on A historical overview on the information technology developments and its implication on data protection legislation is given by the dataprotection.eu.
22. Article on Data Protection Working Party 2009 published by European Union.
23. Article on Data Protection Working Party 2010, published by European Union.
24. Article on Data Protection Working Party 2003, published by European Union.
25. Article on Historical Analysis on European General Data Protection Regulations, published by European Data Protection Supervisor.
26. Analysis of Article 21 of the Constitution- The Expanding Horizons by Vidhan Maheshwari

27. Article on CoE, Committee of Ministers (1973), Resolution (73) 22 on the protection of the privacy of individuals *vis-à-vis* electronic data banks in the private sector, 26 September 1973.
28. Article on CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, CETS No. 108, 1981.
29. Article on CoE, Amendments to the Convention for the protection of individuals with regard to automatic processing of Personal Data allowing the European Communities to accede, adopted by the Committee of Ministers, in Strasbourg, on 15 June 1999; Art. 23 (2) of the Convention 108 in its amended form.
30. Data Protection Directive
31. Agreement on the European Economic Area, OJ 1994 L 1, which entered into force on 1 January 1994.
32. Article 29 Working Party (2010), Opinion 1/2010 on the concept of 'controller' and 'processor', WP 169, Brussels, 16 February 2010, p. 31.
33. Article 29 Working Party (2011), Opinion 15/2011 on the notion of consent.
34. OECD (2013), *Guidelines governing the protection of privacy and transborder flows of personal data*, para. 19 (c).
35. Convention 108, Art. 12 (3) (a).
36. Article 29 Working Party (2011), Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing,
37. European Council's decision of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program.
38. CoE, Committee of Ministers (1995), Recommendation Rec(95)4 to member states on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, 7 February 1995.

39. Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector
40. Article 13 of the amended Directive.
41. CoE, Committee of Ministers (1997), Recommendation Rec(97)5 to member states on the protection of medical data, 13 February 1997.
42. Article 29 Working Party (2007), Working Document on the processing of personal data relating to health in electronic health records (EHR), WP 131, Brussels, 15 February 2007.
43. Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross border healthcare
44. EDPS (2013), Opinion of the European Data Protection Supervisor on the Communication from the Commission on 'eHealth Action Plan 2012–2020 – Innovative healthcare for the 21st century', Brussels, 27 March 2013.
45. Council of Europe, Committee of Ministers (1997), Recommendation Rec(97)18 to member states on the protection of personal data collected and processed for statistical purposes, 30 September 1997.
46. CoE, Committee of Ministers (1990), Recommendation No. R(90)19 on the protection of personal data used for payment and other related operations, 13 September 1990.
47. European Commission (2011), Proposal for a Directive of the European Parliament and of the Council on the access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms and amending Directive 2002/87/EC of the European Parliament and of the Council on the supplementary supervision of credit institutions, insurance undertakings and investment firms in a financial conglomerate, COM(2011) 453 final, Brussels, 20 July 2011.
48. Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ 2007 L 319.
49. Ponnurangam Kumaraguru Et Al., Privacy Perceptions in India and the United States: An Interview Study (2005).

50. Richard A. Shweder & Edmund J. Bourne, *Does the Concept of the Person Vary Cross-Culturally?*
51. "An outbreak of data protectionism?", The economist, September 2nd 2004, available on http://www.economist.com/printedition/displayStory.cfm?Story_ID=3160118
52. Ponnurangam Kumaraguru & Lorrie F. Cranor, *Privacy In India: Attitudes And Awareness, In* PROCEEDINGS OF THE 2005 WORKSHOP ON PRIVACY ENHANCING TECHNOLOGIES (PET 2005: 30 MAY - 1 JUNE 2005, DUBROVNIK, CROATIA).
53. G. GOVINDA and N. SINGH, "The Political Economy of India's Federal System and its Reform", April 2004, p. 2.
54. Notification no. 9(16)/2004 –EC dated January 7, 2005
55. New Indian Privacy and Data Protection Rules, By Vijay Pal Dalmia, Advocate
56. *Privacy & Human Rights, " An international survey of privacy laws and developments ", by Electronic Privacy Information Center, 2004*
57. Danish Jamil & , Muhammad Numan Ali Khan, Data Protection Act in India with Compared to the European Union Countries, International Journal of Electrical & Computer Sciences IJECS-IJENS Vol: 11 No: 06, Available at: http://www.ijens.org/Vol_11_I_06/112206-7474-IJECS-IJENS.pdf.
58. G. GOVINDA and N. SINGH, "The Political Economy of India's Federal System and its Reform", April 2004, p. 2, available on http://repositories.cdlib.org/cgi/viewcontent.cgi?article=1015&context=ucscecon
59. Vidushpat Singhania, Is there a database right protection in India? Lakshmikumaran & Sridharan Attorneys, Available at: http://www.lakshmisri.com/News
60. Arun Agarwal, Need for data protection law, The Hindu, 24th May 2005, http://www.hindu.com/op/2005/05/24/stories/2005052400481700.htm.
61. "Offshore Outsourcing to India by U.S. and E.U. Companies," Barbara Crutchfield George and Deborah Roach Gaut, 6 U.C. Davis Bus. L.J.. 13 (2006).

62. Does India need a separate data protection law?, available at http://www.knspartners.com/files/BNA%20Article-180106.pdf
63. Directive 95/46/EC 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, Art. 14.
64. Want To Buy An IPL Ticket? Better Have An Aadhaar Card! Article by Hemanth Kashyap published in India Times on January 29, 2017, available at https://www.indiatimes.com/sports/want-to-buy-an-ipl-ticket-better-have-an-aadhaar-card-270476.html
65. No Aadhaar? pay Rs. 100 for registration at AIIMS article at The Hindu, available at http://www.thehindu.com/news/cities/Delhi/No-Aadhaar-pay-Rs.100-for-registration-at-AIIMS/article16871186.ece
66. Business Standard, "Aadhaar not mandatory to claim any state benefit, says Supreme Court" March 17th, 2015. Available at: http://www.business-standard.com/article/current-affairs/aadhaar-not-mandatory-to-claim-any-state-benefit-says-supreme-court-115031600698_1.html
67. SSA FAQ "Can I refuse to give my social security number to a private business?" Available at:https://faq.ssa.gov/link/portal/34011/34019/Article/3791/Can-I-refuse-to-give-my-Social-Security-number-to-a-private-business.
68. Dr. Dinoj Kumar Upadhyay, India-EU FTA: Building New Synergies, Indian Council for World Affairs, November 2012, http://www.icwa.in/pdfs/VPIndiaEUTFA.pdf.
69. Deepak Rao, What to expect from the India-EU FTA, http://www.gatewayhouse.in/what-to-expect-from-the-india-eu-fta/
70. India to EU: Declare us a data secure country, Times of India, October 2012, Available at: http://articles.timesofindia.indiatimes.com/2012-10-18/software-services/34554412_1_india-under-data-protection-flow-of-sensitive-data-india-and-eu.
71. How secure are India's call centers- Soutik Biswas, available at http://news.bbc.co.uk/2/hi/south_asia/4619859.stm
72. Data protection and offshoring to India, available at http://www.out-law.com/page-3608
73. Article 8 of the Data Protection Directives.

74. Report of the Group of Experts on Privacy
75. Jürgen Schaaf and Thomas Meyer, Outsourcing to India: Crouching Tiger Set to Pounce (Deutsche Bank Research), Oct. 25, 2005, available at http://www.dbresearch.com/PROD/DBR_INTERNET_ENPROD/PROD0000000000192125.pdf
76. Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data on the free movement of such data (General Data Protection Regulation) Available at: http://ec.europa.eu/justice/data-protection / document / review2012 /com_2012_11_en.pdf. Article 4 and 7
77. Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. Available at: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf
78. Approach paper for a legislation on privacy, published by Government of India, Ministry of Personnel, PG & Pensions Department of Personnel Training on 25th October 2010.
79. India tightens Data Protection law available at http://www.atimes.com/atimes/South_Asia/HJ20Df01.html

2. Case Laws Referred

1. Judgment in All India Reporter 1963 SC 1295
2. Case Discussion of Kharaksingh V. State Of Uttar Pradesh ((1964) SCR (1) 332)
3. Case Report of Govind V. State Of Madhya Pradesh (AIR 1975 SC 1378)
4. Case Report of Rajagopal V. State Of Tamil Nadu (1994 SCC (6) 632)
5. Case Report of PUCL v.s Union of India ((1997) 1 SCC 30)
6. Case Report of AIR 1974 SC 348
7. Case Report of AIR 1999 SC 495
8. Case Report pf District Registrar v. Canara Bank ((2005) 1 SCC 496)
9. Case Report of Peoples Union for Civil Liberties (PUCL) v. Union of India, AIR 2003 SC 2363
10. Case Report of Maneka Gandhi V. Union Of India

11. Case Report of AIR 1992 Ker.351.
12. Mr. X v. Hospital Z, (1998) 8 SCC 296. "The right to privacy is enshrined in Article 21 of the Constitution of India".
13. Case Report of ECtHR, Niemietz v. Germany, 13710/88, 16 December 1992.
14. Case Report of ECtHR, Amann v. Switzerland [GC], No. 27798/95, 16 February 2000, para. 65.
15. Case Report of ECtHR, Amann v. Switzerland [GC], No. 27798/95, 16 February 2000.
16. Case Report of ECtHR, Von Hannover v. Germany, No. 59320/00, 24 June 2004;
17. Case Report of ECtHR, Sciacca v. Italy, No. 50774/99, 11 January 2005.
18. Case Report of ECtHR, Peck v. the United Kingdom, No. 44647/98, 28 January 2003;
19. Case Report of ECtHR, Köpke v. Germany, No. 420/07, 5 October 2010.
20. Case Report of ECtHR, Amann v. Switzerland [GC], No. 27798/95, 16 February 2000, para. 50.
21. Case Report of ECtHR, Amann v. Switzerland [GC], No. 27798/95, 16 February 2000, para. 56.
22. Case Report of ECtHR, Leander v. Sweden, No. 9248/81, 26 March 1987, para. 58.

3. Books Referred :

1. Data Governance : How to design, deploy and sustain an effective Data Governance Programme. by John Ladley.
2. Parag Diwan and Shammi Kapoor., Cyber and E-Commerce Laws with Information Technology Act,2000 & Rules therewith, Bharat Publishing House, New Delhi, 2nd Edition,2000.
3. International Relations, fourth edition book by Peu Ghosh published by Eastern Economy Edition.
4. Data Protection : A Practical Guide to UK and EU Law. by Peter Carey.
5. Book on The Regulation Of Privacy And Data Protection In The Use Of Electronic Health Information, by R. J. Rodrigues, P. Wilson and S. J.

Schanz, published by PAN Health Organization.

6. Indian Public Administration: Institutions and Issues, by Ramesh K. Arora and Rajni Goyal, published by Wishwa Prakashan.
7. Privacy and Data Protection in Business : Laws and Practice. by Jonathan I. Ezar.
8. A Practical Guide to the Data Protection Act. by John Woulds.
9. Data Protection Principles in the Personal Data (Privacy) Ordinance. by Office of the Privacy Commissioner for Personal Data, Hong Kong.
10. Hofstede's Cultural Dimensions
11. Constitution Of India
12. The Information Technology Act, 2000.

4. Websites Referred :

1. http://europa.eu/about-eu/eu-history/index_en.htmEDPS/Legislation
2. http://www.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/Legislation
3. http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&enUSS_01DBC.html#memorandum
4. http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm
5. http://www.coe.int/
6. Federal Data Protection Act (Bundesdatenschutzgesetz,BDSG), available at http://www.iuscomp.org/gla/statues/BDSG.htm.
7. http://conventions.coe.int/treaty/en/Treaties/Html/108.htm
8. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/00/301&format=HTML&aged=0&language=EN&guiLanguage=en
9. www.hindu.com/2007/11/29/stories/2007112954530500.htm
10. http://www.rajeev.in/pages/Rajeev_Bills.aspx
11. http://rajyasabha.nic.in/rsnew/annual_report/2011/bill.pdf
12. http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf
13. http://www.thehindu.com/news/national/article2082643.ece
14. http://computer.financialexpress.com/20040426/coverstory01.shtml

15. http://books.google.co.in/books?id=b3LDI-FBV0AC&pg=PA225&lpg=PA225&dq=Data+Protection+Authority+of+India&source=bl&ots=jxL-LVHSlp&sig=x2HxchU2w_Sc-XmPoA_AuloaWEk&hl=en&sa=X&ei=CpcZUoGLOsP_rQfW9oGICw&ved=0CHIQ6AEwCQ#v=onepage&q=Data%20Protection%20Authority%20of%20India&f=false
16. United Nations (UN), Universal Declaration of Human Rights (UDHR), 10 December 1948, available on www.un.org
17. Decision and Order, Petco Animal Supplies, Inc., FTC File No. 032-3221 (2004) available on www.ftc.gov
18. 20 USC § 1232g, available at http://www.gpo.gov/fdsys/pkg/USCODE-2011-title20/pdf/USCODE-2011-title20-chap31subchapIII-part4-sec1232g.pdf.
19. 15 U.S.C. §§ 6501, *available at* http://www.coppa.org/coppa.htm.
20. http://www.legalarchiver.org/hipaa.htm.
21. http://www.healthit.gov/sites/default/files/hitech_act_excerpt_from_arra.pdf.
22. http://www.gpo.gov/fdsys/pkg/USCODE-2011-title20/pdf/USCODE-2011-title20 chap31
23. http://www.ftc.gov/os/statutes/031224fcra.pdf.
24. http://www.leginfo.ca.gov/cgibin/displaycode?section=fin&group=04001-05000&file=4050-4060.
25. http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001 02000&file=1798.80-1798.84.
26. http://oag.ca.gov/privacy/COPPA.
27. http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf. curia.europa.eu
28. http://www.nasscom.org/artdisplay.asp?cat_id=800
29. http://www.economist.com/printedition/displayStory.cfm?Story_ID=31601 18
30. http://www.cs.cmu.edu/~ponguru/tprc_2005_pk_lc_en.pdf.
31. *http://link.springer.com/chapter/10.1007/978-94-010-9220-3_4?no-access=true*

32. http://Lorrie.Cranor.Org/Pubs/PET_2005.Html;
33. http://repositories.cdlib.org/cgi/viewcontent.cgi?article=1015&context=ucscecon
34. 15 U.S.C. §§ 6501, *available at* http://www.coppa.org/coppa.htm.
35. 20 USC § 6801 available at http://www.gpo.gov/fdsys/pkg/USCODE-2011-title20/pdf/USCODE-2011-title20-chap31 subchapIII-part4-sec1232g.pdf.
36. Indian ITES-BPO Trends (2003-04), available on http://www.nasscom.org/artdisplay.asp?cat_id=800
37. Aapka Aadhaar. Available at: https://uidai.gov.in/aapka-aadhaar.html
38. Social Security Numbers for Noncitizens. Available at: http://www.ssa.gov/pubs/EN-05-10096.pdf
39. Government of India Planning Commission "Notification". Available at: https://uidai.gov.in/images/notification_28_jan_2009.pdf
40. The Social Security Act of 1935. Available at: http://www.ssa.gov/history/35act.html
41. The United States Department of Justice, "Overview of the Privacy Act of 1974". Available at: http://www.justice.gov/opcl/social-security-number-usage
42. UID FAQ: Aadhaar Features, Eligibility. Available at: https://resident.uidai.net.in/faqs
43. History of SSA 1993 - 2000. Chapter 6: Program Integrity. Available at: http://www.ssa.gov/history/ssa/ssa2000chapter6.html
44. Social Security Number Chronology. Available at: http://www.ssa.gov/history/ssn/ssnchron.html
45. Information Technology (Reasonable security practices and procedures and sensitive personal data or information rules 2011) available at: http://deity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf
46. Social Security History 1993 - 2000, Chapter 6: Program Integrity. Available at: http://www.ssa.gov/history/ssa/ssa2000chapter6.html
47. UIDAI, Lost EID/UID Process. Available at: https://uidai.gov.in/images/mou/eiduid_process_ver5_2_27052013.pdf

48. SSA. New or Replacement Social Security Number Card. Available at: http://www.ssa.gov/ssnumber/
49. Social Security available at: http://www.ssa.gov/
50. Aadhaar enrollment/correction form. Available at: http://hstes.in/pdf/2013_pdf/Genral%20Notification/Aadhaar-Enrolment-Form_English.pdf
51. Social Security Administration, Application for a Social Security. Available at: http://www.ssa.gov/forms/ss-5.pdf
52. http://timesofindia.indiatimes.com/india/probe-against-3-firms-for-illegal-use-of-aadhaar-biometrics/articlesshow/57321007.cms
53. https://medium.com/@st_hill/i-wrote-a-few-words-about-aadhaar-34e141afb725
54. OECD Privacy Principle. Available at: http://oecdprivacy.org.

"DATA PROTECTION IN INDIA : A COMPARITIVE STUDY"

A Thesis Submitted To

Nirma University

In Partial Fulfillment Of The Requirements For

The Degree Of

Doctor Of Philosophy

In

Law

BY

SHIVANI JOSHI (11EXTPHDLO2),

Institute Of Law

Nirma University

Ahmedabad – 382481

Gujarat, India.

(August 2019)

CHAPTER 6
CONCLUSION AND SUGGESTIONS

Part 5
Conclusion

Data protection has emerged as an important reaction to the development of information technology. In India data protection is covered under the Information Technology Act, 2000 (hereinafter, the Act). The Act defines 'data' as, "'data' means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer". Protection of such data and privacy are covered under specific provisions in the Act. In the recent past, the need for data protection laws has been felt to cater to various needs. The following analyses the position of data protection law with respect to some of the needs.

In the recent past, concerns have been raised both within the country as well as by customers abroad regarding the adequacy of data protection and privacy laws in the country. A few incidents have questioned the Indian data protection and privacy standards and have left the outsourcing industry embarrassed.

With globalization and increasing BPO industry in India, protection of data warrants legislation. There are reasons for this. Every individual consumer of the BPO Industry would expect different levels of privacy from

the employees who handle personal data. But there have been situations in the recent past where employees or systems have given away the personal information of customers to third parties without prior consent. So other countries providing BPO business to India expect the Indian government and BPO organizations to take measures for data protection. Countries with data protection law have guidelines that call for data protection law in the country with whom they are transacting. For instance, in, the European Union countries according to the latest guidelines, they will cease to part with data, which are considered the subject matter of protection to any third country unless such other country has a similar law on data protection. One of the essential features of any data protection law would be to prevent the flow of data to non-complying countries and such a provision when implemented may result in a loss of "Data Processing" business to some of the Indian companies.

There has been a strong opinion that if India strengthens its data protection law, it can attract multi-national corporations to India. India can be home to such corporations than a mere supplier of services. Apart from this a large data has been collected by the private agencies for Aadhaar card; this Aadhaar number contains personal details of the citizen of India. Hence, protecting Aadhaar number under a stringent law is much more necessary to avoid any disastrous offence which can bring an innocent citizen under severe trouble.

If it was not for this rapidly increasing off-shoring business and the Unique Identification Number programme, India would perhaps never have worried much about data protection, as there are already existing provisions in the Indian legal framework for protection of data, though not at the scale at which protection is warranted under the current circumstances. The Aadhaar number, which is a single global identifier that is supposed to work across application domains, makes individuals vulnerable to privacy breaches. In an Aadhaar like setup, the biggest threat to privacy comes from

potential insider leaks. The Aadhaar programme does not seem to have been explicitly designed to have strong protections against such insider leaks. We believe that effective protection against insider leaks necessarily requires a data controller at UID headquarters as well as at the companies hired for the collection of data on behalf of the government. UID programme has started and various complaints also have been registered against the company hired for collection of data by the government at several places. Thus, though there are serious privacy concerns at present, we believe that Aadhaar can be made safe from the legal perspective by enacting a legal framework for data protection for more specific significant strengthening. Perhaps the single most important specific question that begs answering is who should have the right to verify the identity of an individual, and under what circumstances? Though Aadhaar Act has been enacted but a stringent single codified law is needed for the better protection of data in India.

In 2017 and 2018 status of protection in India was the focal point of numerous discourses. The presence of privacy as one of the fundamental right was confronted by the government before the Supreme Court. Promoters favoring privacy were viewed as differentiating the estimations of Indian culture. Endeavours for framing a separate legislation for data protection were in vein. The most recent judgment of Supreme Court on Aadhaar confronted the manner personal data is protected in India.

On 24 August 2017, a nine-judge bench of the Supreme Court laid down judgment, together upholding that privacy was a fundamental right, retaining individual's nobility and independence and expressing it as the core of the constitutional order. Privacy in this technologically advanced world is no more an extravagance concern; it influences each person as it is pervasive through the mode of web. By the end of July, Justice B. N. Shrikrishna Committee was appointed by the government who came up with a report along with a draft bill for data protection for India.

In spite of the fact that the Draft Bill For Personal Data Protection confined by Justice B. N. Shrikrishna Committee covers serious issues identified with personal data which needs protection, it has still left much hazy area which should be attended too. India is place where diverse languages are method of correspondence utilized by its nationals. There are numerous residents of India who even today has shallow comprehension of Hindi or English. The Draft Bill neglects to address this unpredictable circumstance. Aside from the conceivability of languages another issue that the Draft Bill neglected to address is the issue of lack of education. Huge populace of India is illiterate yet at the same time their data is collected, stored and processed by both government as well as private entities and there are no arrangements made tending to illiteracy.

The Bill suggested by the researcher as outcome of the Ph.D research is been suggested after research carried in various field. There are differences in the Draft Bill suggested by Justice B. N. Shrikrishna and the Bill suggested by the researcher. The researcher has taken care of the language understanding of the citizens of India which The Personal Data Protection Bill, 2018 has failed to address. Another issue which has been taken care of by the researcher in her Bill is illiteracy. The illiteracy rate is high in India and hence it cannot be avoided. For Aadhaar programme data of illiterate people is also collected in the same manner banks, mobile service providing companies and so on collects, store and process the data of illiterate people also. Thus a protection to their data is equally important and their consent for processing of data at the same time is also important. This issue has not been addressed by The Personal Data Protection Bill, 2018.

The researcher has laid the functions to be performed by the Adjudicating Officer which is clear to avoid ambiguity unlike The Personal Data Protection Bill, 2018. The researcher has also suggested notification clause for data managers which is governed by the Adjudicating Officer. This provision is added so that the Adjudicating Officer can know which data

manager is processing what kind of data along with the details of data manager so that he cannot escape easily.

Notification by Data Managers is a chapter added to the Bill suggested by the researcher. This chapter obliges the data manager to make themselves register with the Adjudicating Officer. The notification by the data managers must have details particulars like his name, address and so on of the data manager along with details of the data being processed or the information of data which data manager intends to process. This gives the Adjudicating Officer a chance to have an eye on which data manager is processing what kind of data. This provision can minimize the incidents of data theft or fraud as the Adjudicating Officer would have the knowledge about what data is being processed.

Further the functioning of Data Protection Authority and its office establishment is not made clear in The Personal Data Protection Bill, 2018. However, the researcher has explained those clauses clearly. Further the Draft Bill of researcher has suggested ground level of redressal as every time moving to state tribunal for justice would be costly as well as time consuming for the one's who dwells far from the location of state tribunal. Ground level of redressal has been escaped by The Personal Data Protection Bill, 2018.

Further according to the survey carried out by researcher direct marketing calls, mails, sms, what's app and so on are nuisance to 70% of people who were samples for carrying out the research. 30% of the samples for carrying the research said that the Do Not Disturb application is inefficient as if one has registered with DND still they receive call, sms, etc from various companies. The researcher has made a special provision for direct marketing in her Draft Bill while The Personal Data Protection Bill, 2018 has not explicitly mentioned about direct marketing in whole Bill.

Grievance and Redressal is provided but is not explicit. The role of Adjudicating wing and Adjudicating Officer is not made clear. Moreover, ground level redressal is not clear. A proper system must be set up so that easy and cost effective redressal to the victim is provided. The Draft Bill provides provisions for redressal but proper distribution of the work is not explained in the Draft Bill. The researcher has tried to suggest a law with covers large area of data for protection. Redressal system suggested by the research would solve the issues at district level. Due to this the state level and national level tribunal would not be overloaded with the petitions.

Direct marketing is the much utilized method of marketing in today's time. Indeed, even Banks, educational institutions, tuition classes, mobile companies, online shopping, small shops, eateries, salon, and so forth are utilizing direct marketing to approach their target audience. Direct marketing involves a direct approach to the target audience. This approach incorporates tele-promoting, SMS or mailing to the target audience. Direct marketing might be the most ideal approach to reach target audience, however from the target audience perspective the scene may be contrast. Direct marketing has increased to that extent that DO NOT DISTURB (DND) kind of services has to be initiated. The researcher went to the common people specially educated to get the answer that whether the direct marketing is helpful or is a aggravation. The consequences of the overview led by the researcher were that 70% of the public thought that direct marketing is an annoyance to them. The people involved in direct marketing, calls their target audience at any time hence, it creates nuisance for the people. 30% of people say that though they have registered with the DND service, despite everything they get promoting calls from various organizations. This serious issue has not been addressed by the Draft Bill. No explicit provision has been made for direct marketing. Direct Marketing is the result of lack of data protection. The approach to the target audience direct marketers makes is due to easy flow of data. Such companies collects the data from call centres, other institutions,

and so on paying for the data and then use direct marketing to promote their product or service.

Further the penalty provided to data offender is just 2% of its annual worldwide gain which is not sufficient. Hence the penalty section must be revised and must be marked at such level that anyone needs to think twice before performing data theft or fraud.

FUTURE SCOPE

The study of thesis would lead to better understanding of data protection. The thesis in chapter 4 comes up with the reasons for Indians not much aware about their privacy along with the reasons for such mind set. India believes in developing socially that is together and therefore data protection had never been an issue of discussion in India. Such discussions are found at length in chapter 4 supported by the philosophies given by cultural philosopher. Further, the research reveals that data protection is not only important for Call Centres or BPOs, on the contrary data is being kept in public domain at various other sectors of the business or services. The details discussion of data into public domain with or without the consent or wish of the data subject is at chapter 5 of the thesis. The researcher has tried to suggest a law which is in accordance to Indian needs which depicts the situations and circumstances of India. Any researcher interested to carry his research in the field of data protection would find base and background in this thesis. The law suggested by the researcher is a basic law which can be advanced according to the advancement and development in the technology. Data protection is at the focal point of discussions in India. A codified law would save the private data of the citizens as well as non-citizens which is into public domain and can be misused. A researcher can modify the law in accordance to the need and changes put up by the coming years. As data protection is an emerging area there is much scope of development and alterations into it. A codified law can help Indian Outsourcing Business to new heights which ultimately would result in the economic growth of the country. The Aadhaar which carries biometrics of the citizens of India would be well protected and government would not address any threat to the same which in the interest of citizens India.