

# DATA PROTECTION IN INDIA & EMERGING TECHNOLOGY: NEW CHALLENGES

Ajay Kumar & Ms Arti (Gupta) Ranjan<sup>2</sup>

<sup>1</sup>Associate Professor, <sup>2</sup>Assistant Professor,

<sup>1</sup>Maharishi Law School, MUIT, <sup>2</sup>Noida, School of Data Science, Maharishi University of IT, Noida.

**Abstract:** Data Protection plays a vital role while sharing data using digital methods. It is the process of safeguarding important information from corruption and use by unauthorized user. The purpose of data protection goes beyond merely protecting the personal data that is his/her personal info, it extends to the fundamental rights and freedoms of that person that are related to the data which h has been conferred upon by the Constitution of the country. In this paper need of data protection laws and and data protection laws of India are explained.

## Introduction

Data is a small word but literally comprises the reality of more than half of the world today. With the technology growing day by day and with not only India but the whole world is becoming more and more tech based today, we find that there is lesser of content shared on pages and more through smart phones, laptops, personal computers and the internet. It's not an era of the pigeons brining letters from far flung relatives and not even that of post -cards. It's not an era of letters but of content and data shared making the use of technology. Sometimes we share our personal information, online or offline, without being aware that the share can even be shared publicly with people we might never have heard of. Sharing data has many benefits<sup>1</sup> but with the pros also comes the cons. It is inevitable to be working in today's world without data sharing but it holds a lot of risks. The data if caught in the wrong hands can be exploited to cause irreparable harm to you and hence, the need for robust protection of data is need of hour.

## MEANING OF DATA PROTECTION

Data protection means protecting or safeguarding important information shared through smart phones, internet, laptops and other such devices and means from loss, corruption and from being used without our consent. The significance of data protection is slowly increasing as the amount of data created and stored today is growing at a surprising rate. The term data protection is used to describe both the backup of data which is operational and business continuity or disaster recovery. Data protection strategies are evolving in two forms: data availability and data management. Data availability makes the users assured to have their data they need to practice their everyday business activities even if the data is damaged or lost. Data management includes data lifecycle management. Personal data is any information<sup>2</sup>relating to your private, professional, or public life. On the online platform where wide amount of personal data is shared in the blink of an eye, it is very difficult for people to maintain a check on the personal information they are in fact sharing. This is when the role of data protection comes in.

<sup>1</sup> Accessnow, *Data protection: why it matters and how to protect it*, <https://www.accessnow.org/data-protection-matters-protect/>

<sup>2</sup> Tech target, *Data Protection*, <https://searchdatabackup.techtarget.com/definition/data-protection>

## WHY IS DATE PROTECTION IMPORTANT?

The purpose of data protection goes beyond merely protecting the personal data that is his/her personal info, it extends to the fundamental rights and freedoms of that person that are related to the data which h has been conferred upon by the Constitution of the country.

Not being literate and conscious of regulations governing the data protection regulations can lead to sever financial losses and put you in much harsher situations where a person sitting across the sea can extract all the money from your bank account because you were careless in protecting your personal data.

Organizations that enforces stricter control mechanism with robust check and balances considerably reduce the number of security incidents that result in privacy breaches, implying thereby that the business will and does not lose trust. It also means the business does not have to deal with fines, multi-year penalties, or civil suits as an after effect of breaches, which can be suicidal for these businesses.

## NEED FOR DATA PROTECTION LAWS

The Government should frame detailed data protection legislation and effective legal framework for the following reasons:

- Laws need to be updated: After the internet was invented, people have been making more and more use of the online platform to share their personal information. Privacy rules are a must for the country now and exist and remain important in many countries (Estonia for example) to help protect people's information and human rights. Laws must be updated as per the requirements of the generation now.
- Corporate companies are not working to protect our data. All across the world, be it MNC's, Technology giants, Government entities etc. who do collect people's data for regulation of privacy, hold no or very little responsibility for the legal protection of the data<sup>3</sup>.

## DATA PROTECTION IN INDIA

The 21st century which is commonly known as the information age has witnessed such a sudden and bursting rise in the number of ways in which we use information. India accounts for nearly 450 million Internet users and a growth rate of 7-8% and is well on the path to becoming a digital economy. Taking note of the fact how well digital revolution has permeated India and recognizing its significance, the Government of India has implemented the Digital India initiative. The reality regarding digital environment today is that

<sup>3</sup> Accessnow, *Data protection: why it matters and how to protect it*, <https://www.accessnow.org/data-protection-matters-protect/>.

almost every single conduct which is undertaken by an individual makes use of some sort of data transaction compulsorily. Some of the biggest companies in the world today are data driven companies like Uber, Alibaba, Airbnb etc..... The MNC, Uber holding the world's largest taxi company has no vehicle of its own and Airbnb the world's largest accommodation provider owns no real estate of its own<sup>4</sup>.

## Legal Protection

India has no direct legislation dealing with data protection today. Although a bill known as the Personal Data Protection Bill was introduced in Parliament in 2006, it is yet to be implemented. The bill seems to follow the footsteps of the general framework of the European Union Data Privacy Directive, 1996. It follows a comprehensive model along with the bill with the object of governing the collection, processing and distribution of personal data. As defined in Clause 2 of the bill, it is important to be taken note of that the scope of applicability of the bill is limited to only personal data. The bill applies to both the government and the private corporations involved in data functions. One provision talks about the appointment of persons for the position of data Controllers who hold the responsibility of general superintendence and adjudicatory jurisdiction over subjects mentioned in the bill. It also provides that the punishment sanctions may be imposed on offenders along with the compensation for damages to victims. Even after implementation of data protection law in the country is as close as it could be, still for some reasons the bill is pending<sup>5</sup>.

There are provisions regarding cyber and related IT laws in India in The Information Technology Act, 2000 (IT Act) which also delineates the scope of access that a person can have on data stored on a computer network but nevertheless, the provisions of the act do not emphasise on the urgent need for a data protection law in India. Though the Information Technology Act, 2000 has recently been amended to keep in line with the new upcoming cybercrime challenges, the amended act has yet not come into force. The Act has introduced two important provisions that have a strong meaning on the legality of the data protection and these sections are Section 43A and section 72A of the Information Technology Act. They were inserted but still the provisions pertaining to data security and confidentiality are poorly inadequate.

## Recent amendments to IT Act

Section 43A of IT Act talks about Compensation for failure to protect data. –“Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.” Herein, the term "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities.

<sup>4</sup> Ministry of Electronics and Information Technology (MeitY), *Data Protection In india*, <https://digitalindia.gov.in/writereaddata/files/6.Data%20Protection%20in%20India.pdf>.

<sup>5</sup> Mohammed Nyamathulla Khan, *Does India have a Data Protection law?*, <http://www.legalserviceindia.com/article/I406-Does-India-have-a-Data-Protection-law.html>

Although the meaning of data or information of the term sensitive personal has not been pointed out in the amendment Act and merely states that it would mean such personal information as may be prescribed by the Union government in consultation with such professional bodies or associations as it may deem fit. Section 72 of IT Act is restricted to information obtained by virtue of a power granted under the Information Technology Act. The scope of Section 72A, on the other hand, is wider than the existing one and extends to revealing of personal information of a person without consent while providing services under a legal and lawful contract and not merely to disclosing information obtained by virtue of powers granted under the IT Act<sup>6</sup>.

The term intermediary has been added to section 72A of the Information Technology Act. This has been defined under the amendment Act to mean a person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, Internet service providers, Web-hosting service providers, search engines, online payment sites, online auction sites, online marketplaces and cyber cafes.

### **CONCLUSION : CHALLENGES IN THE FACE OF EMERGING TECHNOLOGY**

In my conclusion, the authors would like to state that it is the most important thing to ensure the protection of the data you have created or are sharing. No matter how much data based work you do, if you are not protecting your data, your work is at a large risk and very unsafe because people who are looking for corrupt practices concerning data are spread all over the internet for making wrongful use of other people's data.

The technology is emerging undoubtedly at the speed of light but in order to be at par with the growing technology, the Government has to take appropriate legal steps and measure to ensure secrecy and security to protect the data of its subjects. There are more and more and newer challenges coming up each day in the country of India due to the technology being increased and lacking in any specific data protection legislation. we might never have heard of. Sharing data has many benefits but with the pros also comes the cons. It is inevitable to be working in today's world without data sharing but it holds a lot of risks. The data if caught in the wrong hands can be exploited to cause irreparable harm to you and hence, the need for robust protection of data is need of hour.

---

<sup>6</sup> ibid