DATA SECRECY AND TEST DATA PROTECTION LAW: A HALF BUILT ROAD IN INDIA

Written by Pooja Devi[1]

ABSTRACT

Data is information and information is the source of knowledge and knowledge is power, then it is very clear for a country to ensure protection against data misappropriation. Data protection refers to the set of laws, policies and practices which aims to minimize the intrusion in one's privacy caused by collection, processing and dissemination of data relates to data subjects. Now the question arises why the data should be protected?In correct manner, which type of data should be protected? There are four categories i.e. personal data, sensitive personal data, confidential business information and test data. As of now, there is no express legislation to protect data from theft or misappropriation in India.

However, there are some provisions in different legislation to protect data up to the limited extent. Protection of confidential business information is governed by contractual relations (confidentiality agreement) between parties under Section 27 of Indian Contract Act.But there is a gap in law to provide remedies in the cases of information misappropriation where confidentiality agreement does not exist. Personal data and sensitive personal data are protected by Section 43-Aand 72-A of Information Technology Act and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.These rules are strict enough but enforcement mechanism is not of such credit.

Though TRIPS agreement provides in Article 39(3) for the protection of test data submitted to government or government agencies for market approvals against unfair commercial use. India being a party has not developed a concrete legal framework yet to protect test data. In the cases of infringement of intellectual property rights lies in the data, collected after the investment of valuable resources,an individual has to invoke common law remedies as provided to protect trade secrets. This situation goes against the innovative efforts in India.

[1]Research Scholar, Kumaun University.

Data Secrecy and Test Data Protection Law: A Half Built Road in India

"No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence."

The Universal Declaration of Human Rights

1. INTRODUCTION

Protecting privacy in the modern era is essential to effective and good democratic governance. However, despite increasing recognition for and awareness of the right to privacy and data protection across the world, there is still a lack of legal and institutional processes and infrastructure to support the protection of rights. Some parts of the world in particular suffer from a void: a lack of regulatory and legal frameworks in many countries, and the poor enforcement in others.[2]

As a result, innovations in policy and technology are largely left unregulated and unchecked, and this will have significant implications for rights of citizens and organisations, as well as for the development of the economies and societies. There is also a systemic and structural challenge which is aggravating this situation. Decision-making and legislative processes are not subject to any or only very limited public scrutiny.

People are increasingly making their personal information available publically. Today there is an unprecedented amount of personal data available to Government and Private Sector Players. Digital India, Aadhaar and Demonetization drives have added to the already growing pool of personal data with various public and private players to pursue their activities. Indian law does not define personal data.

Publically available personal information poses a greater risk to Indians. Individuals are repeatedly transmitting their personal information for various activities. Aspects such as the purpose for collecting personal information, how will this information be used, security mechanisms put in place for protecting such information , for how long will this information be stores, what will be the procedure for destroying such information etc are not known by the individual nor have these aspects been defined uniformly in any law. India's has no specific

[2] Data Protection (Dec.25, 2017, IST 8:15 PM), https://www.privacyinternational.org/topics/data-protection.

legislation focusing on data protection. A few principles of data protection are scattered through IT Act, Guidelines issued by RBI, TRAI etc.

2. DATA PRIVACY

Data privacy, also called information privacy, is the aspect of information technology (IT) that deals with the ability an organization or individual has to determine what data in his possession can be shared with third parties.[3]

Individuals, as citizens and consumers need to have the means to exercise their right to privacy and protect themselves and their information from abuse. This is particularly the case when it comes to our personal information. Data protection is about safeguarding our fundamental right to privacy, which is enshrined in international and regional laws and conventions.

Data protection law is commonly defined as the law designed to protect your personal information, which is collected, processed and stored by "automated" means or intended to be part of a filing system. In modern societies, to empower us to control our information and to protect us from abuses, it is essential that data protection laws restrain and shape the activities of companies and governments. These institutions have shown repeatedly that unless rules restrict their actions, they will endeavor to collect it all, mine it all, keep it all, while telling us nothing at all.

2.1 HOW DOES DATA PROTECTION WORK?

Where a comprehensive data protection law exists, organisations, public or private, that collect and use your personal information have the obligation to handle this data according to the data protection law. This law is based on a number of basic principles[4]. Briefly, these principles require that:

- there should be limits to what is collected: there should be limits on the collection of personal information, and it should be obtained by lawful and fair means, with the knowledge or consent of the individual

[3] An insight into data privacy around the world and the way digital transformation is enabling new legislation, Data Privacy Around the World (Dec.25, 2016, IST 11:15 PM), https://blog.unloq.io/data-privacy-around-the-world-dd30bf2dc6e.

[4]Banisar and David, National Comprehensive Data Protection/Privacy Laws and Bills 2016 (Nov.28, 2016, IST 11:15 PM), https://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416.

- the information should be correct: personal information should be relevant to the purposes for which it is used, should be accurate, complete and up to date;
- there must be no secret purposes: the purposes for which the information is to be used should be specified at least at the time of collection and should only be used for those agreed purposes;
- there must be no creeping purposes: personal information can only be disclosed, used, or retained for only the original purposes, except with the consent of the individual or under law, and accordingly it must be deleted when no longer necessary for that purpose;
- the information must be secure: reasonable security safeguards are used to protect personal information from loss, unauthorised access, destruction, use, modification or disclosure;
- no secret organisations, sources, or processing: we must be made aware of the collection and use of our information, we should know the purpose for its use, and we must know about the organisation that is the data controller;
- individuals have rights to be involved: we should be able to have access to our information, and we must have the right to challenge the information held and to seek its deletion, rectification, completion or modification;
- organisations must be held to account: the organisation that collects and manages your information must be accountable for providing the above principles and rights.

Data protection rules need to be enforced by a regulator or authority, often called a Privacy Commissioner. The strength of the powers invested in these authorities varies from country to country and so does its independence from Government. These powers, for example, can include the ability to conduct investigations, act on complaints and impose fines when they discover an organisation has broken the law.

2.2 WHAT AMOUNTS TO MISAPPROPRIATION?

Collection, processing and dissemination of data without the consent of the data owner and using it for the purpose other than consented amounts to data misappropriation.

2.3 NEED FOR DATA PROTECTION IN THE AGE OF INFORMATION TECHNOLOGY

Every time we use a service, buy a product online, register for email, go to our doctor, pay our taxes, or enter into any contract or service request, we have to hand over some of your personal information. Even without ourknowledge, information about us is being generated and captured by companies and agencies you are likely to have never knowingly interacted with. The only way citizens and consumers can have confidence in both government and business is through strong data protection practices, with effective legislation to help minimise needless monitoring by officialdom and regulate surveillance by companies.

Since the 1960s and the expansion of information technology capabilities, business and government organisations have been storing this personal information in databases. Databases can be searched, edited, cross-referenced and data shared with other organisations and across the world. Once the collection and processing of data became widespread, people started asking questions about was happening to their information once it was turned over. Who had the right to access the information? Was it kept accurately? Was it being collected and disseminated without their knowledge? Could it be used to discriminate or abuse other fundamental rights?

From all this, and growing public concern, data protection principles were devised through numerous national and international consultations. The German region of Hesse passed the first law in 1970, while the US Fair Credit Reporting Act 1970 also contained some elements of data protection. The US-led development of the 'fair information practices' in the early 1970s that continue to shape data protection law today. The UK also established a committee around the same time to review threats by private companies and came to similar conclusions. National laws emerged soon afterwards, beginning with Sweden, the US, Germany and France. Further momentum was added in 1980 when the Organisation for Economic Cooperation and Development (OECD) developed its privacy guidelines that included 'privacy principles', and shortly thereafter the Council of Europe's convention came into force.[5]

While over 100 countries now have laws[6], in many countries there is still a great need for stronger legal safeguards to give citizens and consumer's confidence in what is done to their personal information by government and business. Although most countries have accepted data protection is necessary in selected sectors they have not yet developed comprehensive data protection law that applies to all business sectors and to government.

[5] Data Privacy (Sept. 1, 2017, IST 11:25 PM), https://www.privacyinternational.org/node/44.

[6] Banisar and David, National Comprehensive Data Protection/Privacy Laws and Bills 2016 (Nov. 28, 2016, IST 8:24 PM), https://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416.

3. DATA CATEGORIES IN NEED OF PROTECTION

There are four categories of data that needs statutory protection-

i. PERSONAL DATA-Personal information means any kind of information (a single piece of information or a set of information) that can personally identify an individual or single them out as an individual. The obvious examples are somebody's name, address, national identification number, date of birth or a facial image. A few perhaps less obvious examples include vehicle registration plate numbers, credit card numbers, fingerprints, a computer's IP address, CCTV video footage, or health records. You can be singled out from other people even if your name is not known; for example online profiling companies assign a unique number and use tracking techniques to follow you around the net and build a profile of your behavior and interests in order to present you with advertisements.[7]

ii. SENSITIVE PERSONAL DATA-Some personal information is considered more sensitive than other, and therefore subject to stricter rules; this includes your racial or ethnic origin, political views, religion, health, and sex life. Such information cannot be collected or used at all without your specific consent. [8]

iii. CONFIDENTIAL BUSINESS INFORMATION-Trade Secret in common parlance is 'information of commercial value kept secret'. It could comprise consumer profiles, list of customers and suppliers or may consist of information on distribution networks, advertising strategies or may include information on manufacturing process[9]and technical know-how.

iv. TEST DATA-Test data is the form of data based on information collected for the submission to government or government agencies in fact it is the data of the original marketing authorization holder relating to (pre-) clinical testing and protected under article 39(3) of TRIPS convention.[10]

4. PROTECTIVE LEGISLATIVE APPROACHES TOWARDS DIVERSIFIED DATA CATEGORIES

Data protection in India is governed by loosely constructed provisions of the Information Technology Amended Act, 2008 (ITAA) under Sections 43-A and 72-A of the Act.

[7] Data Privacy (July 16, 2017, IST 11:10 PM), https://www.privacyinternational.org/node/44.
[8] Data Privacy (July 18, 2017, IST 10:35 PM), https://www.privacyinternational.org/node/44.
[9] Adopted from the WIPO website (July 18, 2017, IST 7:25 PM), http://www.wipo.int/sme/en/ip_business/trade _secrets/trade _secrets.
[10] Test data exclusivity (Aug.8, 2017, IST 10:55 PM), https://en.wikipedia.org/wiki/Test_data_exclusivity.

Compensation for failure to protect data (Section 43-A) was introduced by way of an amendment in 2008, which states the liability of a body corporate to compensate in case of negligence in maintaining and securing the "sensitive data." However, the Act fails to define "sensitive data" and states the same as "personal information as may be prescribed by the Central government."

Although three years later, IT Rules 2011 were issued by WIPO defining in detail the term "sensitive data" and what it entails. As the IT Rules issued have been poorly drafted, the applicability of the same has always been in question.

Breach of data privacy has also been mentioned under the ITAA and is punishable under Section 72-A (introduced by an amendment in 2008), which penalises the offender for a three-year imprisonment or a maximum fine of Rs 5 lakh.

The effort to bring in a second legislation — Personal Data Protection Bill — governing data protection and privacy has been in the pipeline since 2006. Several amendments have been made to the Bill and the latest draft was introduced in Rajya Sabha in 2014. This bill provides a small definition of "personal information" and vaguely explains the role of a "Data Controller." Data controller has been defined as those people who view the complaints relating to processing, disclosing of personal data and claim for compensation. Unable to explain the duties and responsibilities of a data controller, the bill also fails to underline the issue relating to outsourced data and the liabilities of companies outsourcing and hosting the data.

The current legislation (ITAA) fails to mention the enterprises that store data and questions their liability in case of a breach and compensation to consumers.

This is all about personal and sensitive personal data which are somehow protected under IT Act and rest two Categories i.e. Test data and confidential business information gets no benefit of statutory protection it is all up to the courts to address the cases relying upon the common law remedies.

5.DATA PROTECTION LAWS IN SELECTED COUNTRIES

Most of the developed countries have enacted strong data protection legislation. There are about 20 data privacy and security laws in the U.S., specific to sectors and mediums, as well as hundreds other such laws across its 50 states and territories.

CANADA has 28 privacy statues that regulate the protection of personal information in the public, private and health sectors, varying in scopes and provisions, but pursuing the same purpose of protection of personal information.Despite its robust approach to data privacy, the People's Republic of China does not have a comprehensive data protection law, but more like rules regarding personal data protection scattered across its legislation.Be that as it may, the base of general data protection rules lie in "The Decision on Strengthening Online Information Protection" and the "National Standard of Information Security Technology—Guideline for Personal Information Protection within Information System for Public and Commercial Services"

JAPAN:After European Union, Japan introduced a separate central legislation for theprotection of data as the Act on the Protection of Personal Information (APPI). The Act took partial effect in 2016 and has been enforceable from May 30, 2017. The law defines the scope of the legislation and states on whom the law is applicable under Article 2-4 of the APPI. As per the Act, it is applicable to four entities- state institutions, local public bodies, independent administrative agencies and an entity not having over 5,000 individuals' personal information for more than six months. Similar to the EU law, consent of a data subject forms the essence of the legislation and has been stated as mandatory in case of transmitting data to a third party or for any use beyond communication purposes.[11]

EUROPEAN UNION (EU): Distinct from all other major human rights documents, protection of people's data has been included as one of the fundamental rights of the European Union under Article 8 of the Charter of the Fundamental Rights of the European Union. Right to privacy and consent of an individual form the basis of Article 8 adding the right to access data and the right to have it rectified.

EU superseded the Data Protection Directive with the General Data Protection Regulation in 2016 and the same Regulation will be enforceable from 2018. The Regulation will be applied to all 28 of the European Union members. Data processors will be held under the law which would include individuals as well as companies processing bulk data.[12]

[11] Sonakshi Avasthi, Data privacy: Where is India when it comes to legislation? (Aug.24, 2017, IST 10:29 PM), http://indianexpress.com/article/india/what-is-india-data-privacy-laws-4811291/.

[12] Sonakshi Avasthi, Data privacy: Where is India when it comes to legislation? (Aug.24, 2017, IST 10:29 PM), http://indianexpress.com/article/india/what-is-india-data-privacy-laws-4811291/.

In order to remove obstacles from thecross-border flow of data, the Directive states that privacy of people and freedom should be maintained at all levels by processing the data equivalent in all Member states.

The European Union Directive 95/46/EU, Data Protection Directive, lays down the liability of data breach on the data controller. According to the provision, any person who has been a subject of adata breach is entitled to compensation from the data controller.[13]

Transparency and increased rights for individuals are common themes for laws around the world, regardless of the countries' levels of Regulation and Enforcement of Data Privacy laws.[14]

When it comes to data privacy, there rarely is a universal law applicable to all countries' legislation. Oftentimes there is a significant discrepancy between data privacy regulation and enforcement harshness, which makes cross-border data transfers burdensome.

6. INTERNATIONAL APPROACH TO PROTECT DATA PRIVACY

Data protection law has become not only a vehicle for protecting citizens and consumers; it has become a gateway to trade. Various international conventions and guidelines have been established in order to ensure that information can circulate around the world without causing too much damage to 'data subjects' and those businesses do not base themselves in countries with the weakest laws. The OECD Guidelines on the Protection of Privacy, first agreed in 1980 and revised in 2013[15], were the pioneer in establishing the data protection principles, adopted by many countries in their legislation. A driving motivation for the OECD Guidelines was to enable protection of privacy while enabling data to flow across borders and opening up markets.

The international instrument with most teeth, however, is the Council of Europe 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of

[13] Sonakshi Avasthi, Data privacy: Where is India when it comes to legislation? (Aug.24, 2017, IST 11:25 PM), http://indianexpress.com/article/india/what-is-india-data-privacy-laws-4811291/.

[14] An insight into data privacy around the world and the way digital transformation is enabling new legislation, Data Privacy Around The World (Aug.14, 2017, IST 10:23 PM), https://blog.unloq.io/data-privacy-around-the-world-dd30bf2dc6e.

[15] OECD work on privacy (Aug.14, 2017, IST 11:59 PM), http://www.oecd.org/sti/ieconomy/privacy.htm#newguidelines.

Personal Data.[16] This has the force of law for the countries that have signed up to it. Countries from outside Europe can sign-up for it, but unfortunately only Uruguay has done so so far.[17]

The EU's 1995 Directive standardised laws to some extent across European Union member states, partly to enable trade within the European market. The Directive required that data could only be sent to foreign jurisdictions if those countries had adequate laws with protections in place. One notable exception, however, is the US which has repeatedly failed to implement a comprehensive law, and the 1974 Privacy Act only applies to the Federal Government, and only protects US citizens and residents.

As an attempt at a quick fix, there's a separate agreement on personal information transfers between the EU and the US – called the Safe Harbor agreement. This arrangement has been heavily criticised by both Privacy International and the European Commission itself, as it is a voluntary and self-regulatory system which is not adequately implemented and not sufficiently enforced. Though the Obama administration had promised to extend the Privacy Act to European citizens and had repeatedly mentioned introducing a comprehensive law, no meaningful action has yet occurred. It is therefore highly problematic that much of the world's information passes through and exists under the jurisdiction of US law, where non-Americans have no rights at all.[18]

The EU and Council of Europe are trying to update their instruments to consider new challenges to privacy and to strengthen protections. These laws were drafted before the rise of internet giants and marketing associations with significant lobbying capabilities; and before the rise of the anti-terrorism policy agenda. As such, government agencies and companies have been working hard to undermine these legal instruments. For instance, over 3000 amendments were introduced in the European Parliament when the draft General Data Protection Regulation was being discussed, some of them introduced by members of the European Parliament who had copied and pasted the amendments from industry lobbyists briefings. The interests in undermining data protection are stronger than ever.

7. CONCLUSION

[16] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Aug.14, 2017, IST 9:27 PM), http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

[17] Data Privacy (July.19, 2017, IST 8:25 PM), https://www.privacyinternational.org/node/44.

[18] Data Privacy (July.27, 2017, IST 8:25 PM), https://www.privacyinternational.org/node/44.

The current variability of protection of data increases the complexity of information managementactivities and may discourage some investment in knowledge development and diffusion.Stakeholders now recognize the need for further reform in the area of data protection laws. Such reforms might include the institution of effective protection in countries India that lack it now; the harmonization of key aspects across countries that now have divergent approaches; and the establishment of minimum norms for protection.

Although India does not have a dedicated law that addresses data protection, yet the analysis of the concept of privacy given in the Adhaarcase by supreme court of India recently brings out the rich and growing jurisprudence on this subject covering the vital themes of definition of data theft, misappropriation and substantive protection remedies and the associated issue of inevitable disclosure in courts. The legal regime has been dynamic to keep pace with the technological changes evident from the promulgation of the Information Technology Act, 2000 and its subsequent amendments that covers theft of confidential information through the electronic route and mandates stiff penalties, damages and imprisonment. But still, India needs a strong legislation to protect all the four categories and proprietary rights thereto.