DATA SECRECY AND TEST DATA PROTECTION LAW: DRIVING ON A HALF-BUILT HIGHWAY

Written by ***Sankalp Malik***

4th Year BBA LLB Student, Amity Law School, Noida

> *"Wherever the real power in a Government lies, there is the danger of oppression. In our Governments, the real power lies in the majority of the Community, and the invasion of private rights is chiefly to be apprehended, not from the acts of Government contrary to the sense of its constituents, but from acts in which the Government is the mere instrument of the major number of the constituents."*
>
> *— James Madison*

INTRODUCTION

In today's world, we no longer "use" technology but we "live" in it. Cultures are not in isolation of economic and technological advancements. The interplay between technological advancement and cultural curiosity is helping to define the information society. The information economy continues to drive Indian commerce.[1] Resources available on the internet are transforming critical sectors of the world and the society, for example healthcare, energy, education, arts and political life.

[1] India's outsourcing industry is expected to earn revenues amounting to $50 billion by 2012. It is also expected to provide direct employment to 2 million workers by 2012. The outsourcing industry in India has grown at more than 30% a year for five years since 2003. India's outsourcing revenue to hit $50 bn, FIN. EXPRESS, Jan. 29, 2008, available at http://www.financialexpress.com/news/indias-outsourcing-revenue-to-hit-50-bn/266661.

In the above-mentioned areas, personal information of individuals and more importantly proper use of such information plays a vital, value – adding role. It is of utmost importance in such a case to establish trust and ensure flexibility. In order for the nation to develop in full pace without facing tough obstacles is it crucial to focus on the efficiency of privacy protection and the laws relating surrounding privacy.

The fundamental right of Privacy underpins several other rights like the freedom of expression[2], association and belief. In other words, these rights are complimentary and would lose their value in case of violation of an individual's privacy. To find out further solutions, it is expedient to understand the core concept of the term "Privacy".

The terms *privacy* and *right to privacy* cannot be easily captured in a definitive language, it has to be ascertained in different ways to best suit the facts and circumstances of a particular situation. Tom Gaiety said[3] 'right to privacy is bound to include body' inviolability and integrity and intimacy of personal identity including marital privacy. Jude Cooley[4] explained the law of privacy and has asserted that privacy is synonymous to 'the right to be let alone'. Edward Shils[5] has also explained privacy is 'zero relationship between two or more persons in the sense that there is no interaction or communication between them, if they so choose'. Warren and Brandeis[6] has very eloquently explained that 'once a civilization has made distinction between the "outer" and "inner" man, between the life of the soul and the life of the body…. The idea of a private sphere in which man may become and remain himself', in other words, the allowance of space for an individual to grow.

[2] Article 19(1)(a), Constitution of India.
[3] Gaiety Gom. Right to Privacy, 12 Harvard Civil Rights Civil Liberties Law Review, P.233.
[4] Cooley, Thomas M. A Treatise on the Law of Torts, 1888, p.29 (2nd ed.).
[5] Shils Edward, Privacy. Its Constitution and Vicissitudes, 31 Law & Contempt Problems, 1966, p.281
[6] Samuel Warren, Louis D Brandeis. The Right to Privacy. Harvard Law Review, 1890, P.193.

ROLE OF FUNDAMENTAL RIGHTS & JUDICIAL INTERPRETATION

Part-III of the Constitution contains a long list of fundamental rights and has very well been described as the Magna Carta of India[7] The aim of having a declaration of fundamental rights is that certain elementary rights, such as right to life, liberty, freedom of speech, freedom of faith and so on, should be regarded as inviolable under all conditions and that the shifting majority in Legislature of the country should not have a free hand in interfering with these fundamental rights.[8] *Justice Untwalia* has compared the Judiciary to "a watching tower above all the big structures of the other limbs of the State" from which it keeps a watch like a sentinel on the functions of the other limbs of the state as to whether they are working in accordance with the law and the Constitution, the Constitution being supreme.[9]

In the informal method of Judicial Interpretation, the constitutional text does not change, but its interpretation undergoes a change.[10] "While the language of the constitution does not change, the changing circumstances of a progressive society for which it was designed yield new and fuller import to its meaning."[11] Since 1978, the interpretative process has entered a very dynamic phase because of judicial creativity. In Maneka Gandhi's Case, the Supreme Court has held that the provisions of Part III should be given widest possible interpretation.[12] Delivering the judgment, Bhagwati, J., said, "The correct way of interpreting the provisions of Part-III is that attempt of the court should be to expand the reach and ambit of fundamental rights rather than to attenuate their meaning and content." It is important to note that the constitution itself super-scribes the general principles of interpretation through Article 367(1), which states that unless the context otherwise requires, the General Clauses Act, 1897 shall apply for the interpretation of this constitution as it applies for the interpretation of an act of the legislature. Courts have held in cases such as *Jugmendar Das vs State*,[13] that not only the

[7] V.G. Ram Chandran- Fundamental Rights and Constitutional Remedies., Vol. 1 (1964), p. 1
[8] A.K. Gopalan v. State of Madras, AIR 1950 SC 27

[9] Union of India v. Sankalchand Himatlal Sheth, AIR 1977 SC 2328

[10] Constitutional Interpretation, Wheare, Modern Constitutions, 146-147 (1964)

[11] Justices Black and Frankfurter, Conflict in the Court, 57.

[12] AIR 1978 SC 597

[13] AIR 1951 All 703

general definitions provided in the General Clauses Act, but also the general rules of construction given therein are also applicable to the constitution.

In *Keshvananda Bharati vs State of Kerala*,[14] the Supreme Court identified the basic structure of the constitution that reflects its true spirit and held that nothing that hurts the basic structure of the constitution, is constitutional. The Supreme Court also delivered that one should give the freedom to the legislature to enact laws, within the framework of the constitution, that ensures the blessings of liberty to be shared with all.

BIRTH OF PRIVACY AS A FUNDAMENTAL RIGHT

It has been argued that the framers of the Indian Constitution rejected the idea of privacy being a part of the Fundamental Rights. Hence, it has been submitted that it outside the preview of being adjudicated under the Constitution as a Fundamental Right. Over the years, inconsistency from two early judgments (the first: *M.P. Sharma v. Satish Chandra, District Magistrate, Delhi*[15] was rendered by a Bench of eight judges and the second, in *Kharak Singh v. State of Uttar Pradesh*[16] was rendered by a Bench of six judges) created a divergence of opinion on whether the right to privacy is a fundamental right.

As we know that law is dynamic in nature, therefore, with change in society certain landmark judgments like *R. Rajagopal v. State of T.N.*[17], *Govind v. State of M.P.*[18] brought change in the realm of privacy in the Indian context. Furthermore, After taking note of the above-mentioned

[14] AIR 1973 SC 1461

[15] AIR 1954 SC 300

[16] AIR 1963 SC 1295

[17] (1994) 6 SCC 632

[18] (1975) 2 SCC 148; 1975 SCC (Cri) 468

cases, the Supreme Court observed in *People's Union for Civil Liberties v. Union of India*,[19] that:

> *"we have, therefore, no hesitation in holding that right to privacy s a part of the right to 'life' and 'personal liberty' enshrined under Article 21 of the Constitution. Once the facts in a given case constitute a right to privacy, Article 21 is attracted. The said right cannot be curtailed except according to the procedure established by law."*

The scope of *'privacy as a fundamental right'* was further widened in *Ram Jethmalani v. Union of India*[20], *Selvi v. State of Karnataka*[21] The right to privacy has been traced in the decisions which have been rendered over more than four decades to the guarantee of life and personal liberty under Article 21 and the freedoms set out in Article 19.

This debate came to an end when a 9-judge bench of the Supreme Court in *K.S. Puttaswamy v. Union of India*[22] unanimously held that the right to privacy is a fundamental right which is ought to be preserved, protected and which gains it's sanctity under Article 21 of the Indian Constitution. Furthermore, it was held that privacy is an intrinsic part of Article 21 and the freedoms guaranteed by Part III of the Constitution.

The question that now arises is that how vital is the protection of data and to prevent any misappropriation leading to the violation of the Fundamental Right.

INSTITUTIONAL PROCESSES GOVERNING DATA SECURITY

Securing protection of privacy in the modern times is a pre-requisite to successful and good governance based administration. However, regardless of expanding acknowledgement for and familiarity of right to privacy and data protection over the world, there is as yet an absence of legitimate and institutional procedures and framework to help the assurance of such rights.

[19] AIR 1991 SC 207, 211

[20] (2011) 8 SCC 1

[21] (2010) 7 SCC 263

[22] (2017) 10 SCC 1

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.[23]

Accordingly, advancements in policy and technological innovations are generally left unregulated and unchecked, and this will have noteworthy ramifications for privileges of residents and associations, and in addition for the improvement of the economies and social orders. There is likewise a fundamental and auxiliary test which is exasperating in this circumstance. Basic leadership and legislative procedures are not subject to any or just extremely constrained open investigation.

Individuals are progressively making their own data accessible publically. Today there is a remarkable amount of individual information accessible to Government and Private Sector Players. Digital India, Aadhaar and Demonetization drives have added to the officially developing pool of individual information with different open and private players to seek after their exercises. Indian law does not define personal data.

Publically accessible individual data represents a more serious hazard to Indians. People are over and again transmitting their own data for different exercises. Viewpoints, for example, the reason for gathering individual data, in what capacity will this data be utilized, security instruments set up for ensuring protection of such data, for what time extent will this data be stored, what will be the methodology for destroying such data and so on are not known by the individual nor have these angles been characterized consistently in any law. India's has no particular enactment focusing on information security. A couple of standards of information security are scattered through IT Act, Guidelines issued by RBI, TRAI and so on.

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

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.[24]

People, as citizens and commercial users, need the way to practice their entitlement to security and shield themselves and their data from mishandling. This is especially the situation with regards to our own personal data. Information insurance is tied in with defending our principal appropriate to security, which is revered in international and local laws and traditions.

Information insurance law is ordinarily characterized as the law intended to ensure the personal data, which is collected, processed and stored via "mechanized/automated" means or expected to be recorded through a filling system. In the present era, to enable us to control our data and to shield us from mishandling, it is fundamental that data protection laws limit and shape the exercises of organizations and governments. These foundations have demonstrated over and over that unless guidelines confine their activities, they will attempt to gather everything, mine everything, keep everything, while at the same time revealing to us nothing by any means.

HOW DOES DATA PROTECTION WORK

In case of availability of comprehensive laws governing data protection, organization both public and private, collecting data from individuals are obliged to appropriate the data according to the data protection laws. This law is based on a number of basic principles which require that:

[24] 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.

- 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
- 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, unauthorized access, destruction, use, modification or disclosure;
- no secret organizations, 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 organization 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;
- organizations must be held to account: the organization that collects and manages your information must be accountable for providing the above principles and rights.

The need of the hour is for the data protection rules to be enforced by a regulatory authority, which is often known as the 'Privacy Commissioner'. The quantum of powers divested in such authorities varies in each nation and so does it independence from the Government. Such powers, for example, can include the ability to conduct investigations, act on complaints and impose fines when they discover any misappropriation or mis-utilization of data.

WHAT AMOUNTS TO MISAPPROPRIATION?

Accumulation, handling and dispersal of information without the assent of the information proprietor and utilizing it for the reason other than agreed adds up to information misappropriation.

NEED FOR DATA PROTECTION IN THE AGE OF INFORMATION TECHNOLOGY

Each time we utilize a service, purchase an item online, enrol for email, go to our doctor, pay our taxes, or enter into any agreement or policy request, we need to hand over a portion of our own data. Indeed, even without our knowledge, data about us is being created and captured by organizations and offices with which we never purposely collaborate with. The main way residents and customers can believe in both government and business is through solid data protection practices, with compelling enactments to help limit unnecessary checking by officials and control observation by organizations.

Since the 1960s and the advancement of data innovation capacities, business and government associations have been storing away individual data in databases. Databases can be searched, altered, cross-referenced and information imparted to different associations and over the world. Once the accumulation and handling of information became far-reaching, individuals began to make inquiries about was going on to their data once it was turned over. Who had the privilege to get to the data? Is it safe to say that it was kept precisely? Is it true that it was being gathered and spread without their insight? Might it be able to be utilized to segregate or manhandle other fundamental rights? From this, and developing open concern, information assurance standards were contrived through various national and global meetings. The German district of Hesse passed the main law in 1970, while the US Fair Credit Reporting Act 1970 likewise contained a few components of information assurance. The US-drove improvement of the 'reasonable data practices' in the mid-1970s that keep on shaping information security law today. The UK likewise settled an advisory group around a similar time to audit dangers by privately owned businesses and arrived at comparable conclusions. National laws rose soon a short time later, start with Sweden, the US, Germany and France. Further momentum was added in 1980 when

the Organization 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.[25]

While over 100 countries now have laws[26] in numerous nations, there is as yet an incredible requirement for stronger lawful shields to give nationals and buyer's trust in what is done to their own data by government and business. Albeit most nations have acknowledged information insurance is vital in chosen segments they have not yet created exhaustive information security law that applies to all business areas and to government

CATEGORIES OF DATA WHICH NEED TO BE PROPERLY PROTECTED

There are four categories of data in respect of which proper legislative provisions need to be implemented:

i. **PERSONAL DATA**:

Individual data implies any sort of data (a solitary snippet of data or an arrangement of data) that can by and by recognize an individual or single them out as a person. The undeniable illustrations are some person's name, address, national distinguishing identification number, and date of birth or a facial picture. A couple of maybe more subtle cases incorporate vehicle enlistment plate numbers, Visa numbers, fingerprints, a PC's IP address, CCTV video film, or healthcare 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.[27]

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

[26] 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.

[27] Data Privacy (July 16, 2017, IST 11:10 PM), https://www.privacyinternational.org/node/44.

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.[28]

iii. **CONFIDENTIAL BUSINESS INFORMATION:**

Trade secrets in ordinary course refers to 'data of business value which is kept secret'. It could involve buyer profiles, rundown of clients and providers or may comprise of data on dissemination systems, promoting techniques or may incorporate data on manufacturing procedure[29] and specialized 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.[30]

PROTECTIVE LEGISLATIVE APPROACHES TOWARDS DIVERSIFIED DATA CATEGORIES

The greater part of the developed nations have established solid data protection laws. There are around 20 information protection and security laws in the U.S., particularly to areas and mediums, and also hundreds other such laws over its 50 states and domains.

[28] Data Privacy (July 18, 2017, IST 10:35 PM), https://www.privacyinternational.org/node/44

[29] Adopted from the WIPO website (July 18, 2017, IST 7:25 PM), http://www.wipo.int/sme/en/ip_business/trade _secrets/trade _secrets.

[30] Test data exclusivity (Aug.8, 2017, IST 10:55 PM), https://en.wikipedia.org/wiki/Test_data_exclusivity.

CANADA has 28 protection statues that direct the protection of individual data in the general population, private and healthcare areas, fluctuating in degrees and arrangements, however seeking after a similar purpose of protecting an individual's information. Despite its hearty way to deal with information protection, the People's Republic of China does not have an exhaustive information assurance law, but rather more like guidelines in regards to individual information security scattered over its legislation. Be that as it might, the base of general information assurance rules lie in "The Decision on Strengthening Online Information Protection" and the "National Standard of Information Security Technology—Guideline for Personal Information Protection inside Information System for Public and Commercial Services"

JAPAN: After European Union, Japan presented a different focal enactment for the protection of information as the Act on the Protection of Personal Information (APPI). The Act produced incomplete results in 2016 and has been enforceable from May 30, 2017. The law characterizes the extent of the enactment and states on whom the law is relevant under Article 2-4 of the APPI. According to the Act, it is pertinent to four substances state foundations, nearby open bodies, free managerial organizations and an element not having more than 5,000 people's close to home data for over a half year. 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.[31]

EUROPEAN UNION (EU): Distinct from all other significant human rights records, assurance of individuals' information has been incorporated as one of the major privileges of the European Union under Article 8 of the Charter of the Fundamental Rights of the European Union. Appropriate to protection and assent of an individual frame the premise of Article 8 adding the privilege to get to information and the privilege to have it redressed.

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

[31] 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/.

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.[32]

Keeping in mind the end goal to expel hindrances from the cross-outskirt stream of information, the Directive expresses that protection of individuals and flexibility ought to be kept up at all levels by preparing the information equal 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 a data breach is entitled to compensation from the data controller. 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.[33]

With regards to information security, there rarely is an all-inclusive law appropriate to all nations' enactment. As a rule, there is a critical error between information security direction and implementation cruelty, which makes cross-outskirt information exchanges difficult.

CONCLUSION

The present inconstancy of security of information builds the unpredictability of data administration exercises and may dishearten some interest in learning advancement and dissemination. Partners currently perceive the requirement for additionally change in the zone of information insurance laws. Such changes may incorporate the foundation of compelling assurance in nations India that need it now; the harmonization of key angles crosswise over nations that presently have disparate methodologies; and the foundation of least standards for security.

[32] 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/.

[33] 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

In spite of the fact that India does not have a committed law that tends to information assurance, yet the examination of the idea of security given in the Adhaar case by preeminent court of India as of late draws out the rich and developing law regarding this matter covering the indispensable topics of meaning of information robbery, misappropriation and substantive insurance cures and the related issue of inescapable revelation in courts. The legitimate administration has been dynamic to keep pace with the innovative changes clear from the declaration of the Information Technology Act, 2000 and its resulting revisions that spreads robbery of classified data through the electronic course and orders solid punishments, harms and detainment. Yet at the same time, India needs a solid enactment to secure all the four classifications and exclusive rights thereto.