DRIVING DATA: A STUDY ON DATA PROTECTION & PRIVACY LAWS

Written by ***Shaunak Deshpande***

2nd Year BBA LLB Student, Symbiosis Law School Nagpur, Maharashtra

ABSTRACT

Data is an asset in the 21st Century where Information rules the world. In this modern age Data is the Driving force behind the growth of world. With many Gigabytes of data being transported every second throughout the world it becomes necessary to regulate the flow of data. Lot of this data that flows over the internet contains sensitive personal data which is analyzed by companies, hackers and organizations to make some monetary benefits out of it. We as the people that generate this data certainly need a security as to the way in which this generated data is processed or used. We need transparency as to the way our data is accessed. This is where Data Protection Laws comes into the picture. These laws are being enacted upon by many countries for the protection of data that is generated by their citizens.

My research paper discusses the current situation of Data protection Laws in India & around the world it also focuses on the Indian Jurisprudence aspect of Data Protection & privacy. This Research Paper will provide you with the state of Data Protection & Privacy Laws that regulate the way data is processed, analyzed and used

Keywords: Data Protection, Privacy, Laws, Personal Data, Data Theft

INTRODUCTION

Data surrounds us in our day to day lives with every action that we perform even a single word typed is a kind of Data. Whether we travel, order a meal or use transportation we keep on generating data consciously or unconsciously. In this 21st century where data is driving growth, Data has become immensely valuable. In the new age of cheaper Internet, data has become a new currency for exchange. What is even more intriguing that the full potential of the data is not known to the world. As technology progresses, newer applications emerge it keeps on enhancing the value of the data in our lives. With this ever-increasing value of Data, it has become important to protect our valuable data. Jurists around the world are struggling to marry traditional concepts of the law and the absurdly invasive times of data theft that we find ourselves in. Safeguards are necessary to give citizens of the country and consumers deep trust in administration, business and other private entities.

THE CONCEPT OF DATA?

Section 2(1)(o) of the Information Technology Act, 2000 (known as "IT Act") has defined "data" as "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."[i]The electronic consent framework issued by the Digital Locker Authority defines 'data' to mean "any electronic information that is held by a public or private service provider (like a government service department, a bank, a document repository, etc. This may include both static documents and transactional document."[ii]

Personal Data

The Data or the Information that relates to a certain person or makes it identifiable with a person is a personal Data. Personal Data includes attributes regarding a specific natural person. Personal data is anything that can be double checked identify a specific individual. Different pieces of information when collected which can identify with a person can also be called a

personal data. A Personal Data will include things like Your Name, Address, Email Address, Phone number, Aadhar card number, your IP address or something like the health record held by a doctor or a hospital.

Personal Data presents a great deal of commercial value in the market and that is why Personal Data of people is traded for monetary gains by many companies. Therefore, countries around the world are developing legislations to protect this Personal Data.

Privacy of Data

Over the years there has been exponential growth in the amount of data that is generated by users. Today's business generates huge amount of value by analyzing data that we generate. But the main problem that lies ahead is do we have a control over the data that we generate and the way it is to be accessed and processed.

Privacy is the right to be left alone or to be free from misuse or abuse of one's personality. The right of privacy is the right to be free from unwarranted publicity, to live a life of seclusion, and to live without unwarranted interference by the public in matters with which the public is not necessarily concerned.[iii]When the data that has to be kept safe gets in wrong hands, bad things can happen. A data breach at government organization for example can put top secrets into enemy's hands. Privacy is not a new concept. Privacy is a common law concept and an invasion of privacy gives a right to the individual to claim tort-based damages.

Data Theft

Data Theft is when data is transferred illegally from one computer to the other to gain benefits or access to some private & sensitive information of the people. It is considered as a serious breach of privacy and data. The consequences of data theft can be severe for businesses and individuals. Common modes of data theft are through USB Drive, Email, Remote sharing & Malware Attacks

Ways to Prevent Theft

- Use Strong Passwords
- Install Firewall System
- Secure your Wireless Network

- Encrypt your Data
- Make sure your system is up to date
- Train your employees for protection against data theft
- Properly handle & dispose Sensitive data

RULES THAT ARE CURRENTLY GOVERNING DATA PROCESSING AND PROTECTION IN INDIA

As on date the current framework for data protection has been set out in the Information Technology Act 2000(IT Act) and the rules issued under Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("IT Rules")

As Per Sec.43A of IT Act where anybody corporate possessing, dealing or handling any sensitive personal data or information in a computer resource that he owns controls or operates is negligent in maintaining and implementing reasonable security practices and procedures causes wrongful loss or wrongful gain to any person, such body corporate will be held liable to pay damages by way of compensation to the person so affected.

Sec 66A this Act deals with identity theft and states that anyone who fraudulently or dishonestly makes use of digital signature , password or any other unique identification feature of any other person shall be punished with imprisonment for a term of three years and shall also be liable to pay a fine up to Rs.100000(one lakh rupees).

Sec.75 of IT Act stipulates that provisions of IT Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting such offence or contravention involves a computer, computer system or a computer network located in India. The scope of section 69 of the IT Act 2000 includes both interception and monitoring along with decryption for important purposes of investigation of cyber-crimes in India. The Government has also notified the Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, under this section. The Government has notified the Information Technology (Procedures and Safeguards for Blocking for Access of Information) Rules, 2009, under section 69A of the IT Act, that deals with the

blocking of websites. The Government has blocked the access of many websites under this rule. The IT rules that were framed in 2011 require body corporates that are holding sensitive personal information of users to maintain certain specified standard of security for protecting data from theft.

INDIAN JURISPRUDENCE ON DATA PROTECTION AND PRIVACY

Article 21: - Article 21 of the Indian Constitution provides that "No person shall be deprived of his life or personal liberty except according to the `procedure established by law"[iv]However, the Constitution of India does not specifically recognize 'right to privacy' as a fundamental right. This issue has been raised before the judiciary many times and the judiciary has had different opinions on different cases. Whether right to privacy is a part of Article 21 was raised up in the case of *M. P. Sharma and Ors. V Satish Chandra, District Magistrate, Delhi and Ors*.[v] However, in this case Supreme Court refrained from giving right to privacy as a fundamental right.

In the case of *R. Rajagopal and Anr. V State of Tamil Nadu* Supreme court observed that "*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"*[vi]

Subsequently in the case of *People's Union for Civil Liberties (PUCL) v Union of India* the Supreme Court said that *"We have, therefore, no hesitation in holding that right to privacy is 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 procedure established by law"[vii]

This issue was raised again in one of the landmark judgements in the case of *K. S. Puttaswamy (Retd.) v Union of India* the court in this case said that*" Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution. Elements of privacy also arise in varying contexts from the other facets of*

freedom and dignity recognized and guaranteed by the fundamental rights contained in Part III''[viii]

This judgement is the latest judgement to rule out that right to Privacy is a fundamental right. With the judiciary recognizing right to privacy as a fundamental right we are certainly steeping in the right direction towards establishing a system that is designed in a way to protect personal data theft. As a consequence of this judgement many things like "Aadhar card" are now evaluated and ensured that the valuable data of people is kept private free from any breaches. Data at many other government offices is also evaluated and kept safe and this is a significant step in the right direction.

Personal Data Protection Bill 2019[ix]

The judgement in *K. S. Puttaswamy (Retd.) v Union of India* led to the formulation of Personal Data Protection Bill which is currently a draft legislation on Data Protection in India. The bill was introduced in the lower of the parliament on 11th December 2019. It is yet to be passed by Parliament but gives us a fair bit of idea about the progress about data protection laws in India. This Bill aims to regulate the processing of personal data of individuals by government organizations and private entities that are incorporated in India and abroad. Processing of Data is only allowed if the individual gives a consent to do so or in case of medical emergency or by the State for providing benefits to its citizens.

The individual will have several rights with respect to their data such as seeking correction or seeking access to the data that is stored with the private entities. The bill allows exemptions in certain kinds of data processing such as processing in interest of national security, for legal proceedings etc. It also makes it mandatory to store a copy of data within the territory of India. Certain critical personal data must be stored solely in India.

A national level Data Protection Authority (DPA) is set up under the Bill to supervise and regulate data fiduciaries. Under this Bill the DPA can levy penalties on data fiduciaries for failure to comply with 1) data processing obligations 2) directions issued by DPA and 3) cross border data storage and transfer requirements. Failure to promptly notify DPA can attract a penalty higher than 5 crore rupees. Further any person who discloses, obtains, transfers or sells or offers to sell personal sensitive data shall be punishable with imprisonment ranging up to five years or a fine up to three lakh rupees.

Critical Analysis of the Data Protection Bill 2019

Though the bill provides a skeletal framework for data protection and attempts at protecting data yet it suffers from major loopholes. The Data Protection Bill places the obligation on data fiduciaries to collect data in a fair and reasonable manner that which respects the privacy of the individual but the bill does not state or explicitly specify what constitutes fair and reasonable manner of personal data processing which could result in fairness and reasonability principles to vary across data fiduciaries and processing similar types of data an in the same business may evolve and follow different fairness and reasonability standards. India needs to also invest and enhance data center infrastructure available in the country, Internet connectivity and grid capacity before mandating data localization so that its feasible even for smaller organizations to comply with data localization.

The Bill gives a discretionary power to the Data fiduciary on reporting data breaches and to determine if the data breach has caused the data principal any harm. This could result in choosy reporting of data breaches by data fiduciaries which will avoid the DPA from being triggered even when a data breach involves some personal data of an individual. The Bill also does not provide for definitions of some important terminologies. It is uncertain what is meant by a 'serving copy' of data. Furthermore, what is covered within the ambit of 'critical personal data' is not clearly mentioned. It is an important prerequisite for data fiduciaries to prepare in storing this data solely within the territory of India

WHAT IS HAPPENING ACROSS THE WORLD?

Article 12 of the Universal Declaration of Human Rights states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[x]

Article 17 of the International Covenant on Civil and Political Rights (ICCPR) states that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation." [xi]

According to UNCTAD (United Nations conference on Trade and Development) 107 countries (out of which 66 are developing economies) have put in place legislation to secure data and privacy. Globally there are an increasing growth in data protection laws many of these laws have comprehensive guidelines-based framework.[xii]

Canada: - Canada has enacted PIPEDA (The Personal Information Protection and Electronic Documents Act). It mandates business using data in course of commercial activities must disclose the purpose of data collection to the owners of the data and obtain consent to proceed.

USA: - CalOPPA (California online Privacy Protection Act) which was enacted in 2004 broke the ground in USA and made it mandatory for websites to post privacy policies detailing data collection and its use. A new legislation namely CCPA (California Consumer Privacy Act) will be enacted from the year 2020.It demands that companies inform users of data processing and take extra measures to protect user information.

European Union: - European Union has one of the strictest Data protection regimes with GDPR (General Data Protection Regulation). It is based on the principle of consent, transparency, protection and user control and threatens fine as high as 4% of company's annual revenue.

Another legislation that is in place in European Union is the ePrivacy Directive & Regulation which requires that websites obtain user consent to non-essential cookies before launching them.

South Africa: -South Africa has enacted POPI (Protection of Personal Information Act) in 2014.It sets standard for responsible data processing and establishes requirement of customer consent to direct marketing outreach.

China: -China has enacted on Cyber Security Law in 2017.It standardizes Data Protection in China and helps keep sensitive data of Chinese people safe.

Australia: -Although Australia's Privacy Act was enacted in 1988 it has brought up some significant amendments to the same act and has made it better for the citizens. It establishes Information Privacy Principles (IPPs) for Australian Citizens and regulates the data collection by government organizations & companies

Philippines: - Philippines has set data protection laws in the form of Data Privacy Act of 2012.It is applicable to all business that process data of Philippine citizens and residents. It is centered on the principle that data processing should be transparent, proportional and based on legitimate purpose for all.

Germany: - Germany has a strict regime of BDSG (Bundesdatenschutzgesetz). It sets rigid standards under which business are required are required to adopt and maintain protective measures for data stored in IT systems.

Argentina: -It finalized PDP (National Directorate of Personal Data Protection) and has upped the ante considerably for data privacy. It gives for the first time right to request deletion and transfer of their data.

In this way all the major economies of the world are enacting new rules and legislations for data protection and privacy to protect the valuable personal data of its citizens. Which is Intern helping attain a better and a data protected world.[xiii]

Analysis and Suggestions: -The need for data protection laws is felt by everyone around the world. People want security of their personal sensitive data. This is why Data protection laws are gaining momentum throughout the world. People are striving and making government act upon newer data protection laws that provide the people with more transparency and security of their personal sensitive data. The Indian System is trying to enact data protection laws and a draft bill has been already framed but there is need to bring this bill to the parliament and codify it at the earliest is the need of the hour. While we might enact laws throughout the country but it is also important that the citizens of the country are "data aware" citizens who know the way in which their data is being used by many companies for their monetary benefits. With the changes in technologies it will also become necessary for us to amend these data protection laws regularly while keeping its rigidity intact. After having analyzed laws from other countries as well I feel the European GDPR sets a Gold standard as to Data Protection Laws. It also levies heavy fines on companies that do not take necessary measures to protect the data of its citizens. While there are a substantial number of countries that have enacted laws for data protection and privacy but still many nations of the world are still do not have a legislation for protection of data of its citizens. It is certainly the right time for these countries to draft and put in force legislation for data protection.

The current regulations that are provided under IT Act are certainly not enough for the people in India. With India having such a large population it becomes difficult to regulate all the data that is generated by the citizens. In the times where data breaches are happening everyday India must provide security for protection of personal sensitive data of its citizens by enacting law that are well covered with the threats arising out of new technologies. For the effective implementation of the data protection regime it is important that all stakeholders Align their policies with requirements of Data Protection, encourage adoption of Privacy and Explore the possible Consent requirements at the time of data collection

CONCLUSION

Data is going to become more valuable day by day with the exponential increase in the way people consume and generate data around the world. With Data fuelling growth it will be quite important to protect data of the citizens. Governments around the world will have to keep up with the rapidly changing technologies and amend and develop new laws that protect the sensitive personal data of the people. A coordinated effort between the government and it's "data aware" citizens will make this world a better "data secure" world which is transparent and receptive to new policies and laws.

BIBLIOGRAPHY

Statues and Rules

1) THE INFORMATION TECHNOLOGY ACT, 2000 Available at: - https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf
2) The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 Available at: - https://www.prsindia.org/uploads/media/IT%20Rules/IT%20Rules%20Subordinate%20committee%20Report.pdf
3) The Constitution of India 1949, Available at: - https://indiankanoon.org/doc/1199182/

4) Personal Data Protection Bill 2019 Available at: - https://bit.ly/2YdkAm4
5) Universal Declaration of Human Rights Available at: - https://www.un.org/en/universal-declaration-human-rights/
6) International Covenant on Civil and Political Rights Available at: - https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf
7) Electronic Consent Framework-Digital Locker Authority Available at: - https://bit.ly/2YHTySL

Case Laws

1) *Strutner v. Dispatch Printing Co*., 2 Ohio App. 3d 377 (Ohio Ct. App., Franklin County 1982 Available at: - https://bit.ly/3frarb1
2) *M. P. Sharma and Ors. V Satish Chandra, District Magistrate, Delhi and Ors 1954 AIR 300; Available at: - https://indiankanoon.org/doc/1306519/*
3) R. Rajagopal and Anr. V State of Tamil Nadu 1995 AIR 264; Available at: - https://indiankanoon.org/doc/501107/
4) People's Union for Civil Liberties (PUCL) v Union of India AIR 1997 SC 568; Available at: - https://indiankanoon.org/doc/31276692/
5) K. S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1; Available at: - https://indiankanoon.org/doc/127517806/

Other Articles and websites

1) Data Protection in India Available at: - https://digitalindia.gov.in/writereaddata/files/6.Data%20Protection%20in%20India.pdf
2) Data Protection & Privacy Issues in India Available at: - http://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf
3) Multidimensional Approach to Data Protection Laws in India, Loopholes and Solutions: - https://blog.ipleaders.in/data-protection-laws-india-loopholes-solutions/
4) Data Protection and Privacy Legislation Worldwide Available at: -

https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

5) DATA PROTECTION LAWS OF THE WORLD Available at: - https://www.dlapiperdataprotection.com/

REFERENCES

[i] Information Technology Act, 2000 Section 2 cl.1(o); https://indiankanoon.org/doc/1752240/
[ii] Electronic Consent Framework-Digital Locker Authority; https://bit.ly/2YHTySL
[iii] *Strutner v. Dispatch Printing Co*., 2 Ohio App. 3d 377 (Ohio Ct. App., Franklin County 1982).; https://bit.ly/3frarb1
[iv] The Constitution of India 1949 Article 21; https://indiankanoon.org/doc/1199182/
[v] *M. P. Sharma and Ors. V Satish Chandra, District Magistrate, Delhi and Ors 1954 AIR 300; https://indiankanoon.org/doc/1306519/*
[vi] R. Rajagopal and Anr. V State of Tamil Nadu 1995 AIR 264; https://indiankanoon.org/doc/501107/
[vii] People's Union for Civil Liberties (PUCL) v Union of India AIR 1997 SC 568; https://indiankanoon.org/doc/31276692/
[viii] K. S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1; https://indiankanoon.org/doc/127517806/
[ix] Personal Data Protection Bill 2019; https://bit.ly/2YdkAm4
[x] Article 12 Universal Declaration of Human Rights; https://www.un.org/en/universal-declaration-human-rights/
[xi] Article 17 International Covenant on Civil and Political Rights; https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf
[xii] https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx
[xiii] https://www.dlapiperdataprotection.com/