

Data Sharing Policy: A threat to Right to Privacy

Kiran Rai¹

Department of Law, Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh, India¹

kiran.rai@galgotiasuniversity.edu.in¹

ABSTRACT: In the 21st Century, data is an asset where information rules the world. In this modern age, the driving force behind the world's growth is data. It is important to control the flow of data with several gigabytes of data being transported every second around the world. A lot of this information streaming over the internet involves confidential personal data analyzed by corporations, hackers and organizations to make any monetary advantages out of it. As individuals who produce this information, we definitely need a protection as to how this generated data is processed or used. As for the way our data is accessed, we need transparency. This is where the legislation on data protection comes into the picture. Many countries are enacting these laws for the safety of data produced by their people. This study paper examines the current situation of Data Protection Laws in India and around the world and also focuses on the Data Protection & Privacy aspect of Indian Jurisprudence. This review paper will give you the state of the Data Security & Privacy Laws that govern the collection, analysis and use of information.

KEYWORDS: Data Protection, Privacy, Laws, Personal Data, Data Theft.

I. INTRODUCTION

Data fills us with every move we do, even a single word typed, in our everyday lives, is a kind of data. If we fly, order a meal or use transport, we continue to consciously or unconsciously produce data. Data has become incredibly important in the 21st century, where data is driving growth. Data has become a modern currency for exchange in the new era of the cheaper Internet. What is even more intriguing being that the world is not aware of the full potential of data[1].

When technology advances, new technologies begin to develop, increasing the importance of data in our lives. With this ever-increasing importance of data, securing our precious data has become critical. Jurists around the world strive to marry conventional law principles and the absurdly intrusive times of data theft in which we find ourselves. Safeguards are important to have a deep trust in the government, company and other private institutions for the people of the country and consumers[2].

II. THE CONCEPT OF DATA

Data" has been defined by Section 2(1)(o) of the Information Technology Act, 2000 (known as the "IT Act") as "a representation of information, knowledge, facts, concepts or instructions that are being prepared or prepared in a formalized manner and are intended for transmission, processing or processing in a computer system or computer network and may be in any form (including computer network). The Digital Locker Authority's electronic consent framework defines' data 'as "any electronic records kept by a public or private service provider (such as a government service agency, a bank, a document archive, etc. Which may include both static and transactional documents[3].

Personal Data

Personal data is the data or information that relates to a certain entity or makes it visible to a person. Personal data contains characteristics related to a particular person. Personal information is something that a single person can be double-checked to recognize. A personal data may also be called different pieces of information when collected that

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

can associate with an individual. Such details as your name, address, email address, phone number, Aadhar card number, your IP address or something like the health record kept by a doctor or hospital will be included in A Personal Data. Personal data presents a great deal of economic value in the market and that is why many businesses exchange personal data of individuals for monetary profits. Countries around the world are now creating legislation to safeguard this personal information[4].

Privacy of Data

Over the years, the amount of data produced by users has increased exponentially. Today's organization creates tremendous value through the study of the data we produce. But the key challenge that lies ahead is that we have control over the information we produce and how to access and process it.

The right to be left alone or to be free of misuse or exploitation of one's personality is privacy. The right to privacy is the right to be free from unjustified publicity, to live a life of seclusion, and to live without the media's unjustified intrusion in matters which are not actually of interest to the public. If the information that needs to be held secure gets into the wrong hands, bad things can happen. For example, a data breach at a government agency may bring top secrets into the hands of the enemy. Privacy isn't a modern idea. Privacy is a principle of common law and an infringement of privacy gives the person a right to seek tort-based damages[5].

Data Theft

Data theft is when data is secretly moved from one device to the other in order to obtain advantages or access to those people's private & confidential information. It is perceived to be a serious privacy and data breach. For organizations and people, the effects of data theft can be serious. Using USB Drive, Email, Remote Sharing & Malware Attacks are common data theft modes.

III. RULES CONCERNING DATA PROCESSING AND PROTECTION IN INDIA

The current data protection policy has been set out in the Information Technology Act 2000(IT Act) and the regulations provided under the Rules of 2011 ('IT Rules') on Information Technology (Reasonable Security Policies and Procedures and Confidential Personal Data or Information).

As per Sec.43A of the IT Act, if any business that owns, manages or handles any confidential personal data or information in a computer resource that it regulates or operates is negligent in maintaining and enforcing fair security practices and procedures that cause any person to lose or benefit wrongfully, such company will be held responsible for paying damages through compensation[6].

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

Section 75 of the IT Act provides that an offense or contravention committed outside of India by any person is subject to the provisions of the IT Act if the act or conduct constituting such an offense or contravention includes a device, computer system or computer network located in India. The scope of Section 69 of the IT Act 2000 involves both interception and surveillance, as well as decryption of cybercrime investigations in India for important purposes. The Government has also notified, under this clause, the 2009 Rules on Information Technology (Procedures and Safeguards for the Interception, Monitoring and Decryption of Information)[7].

Under section 69A of the IT Act, the Government has notified the Information Technology (Procedures and Protections for Blocking Access to Information) Rules, 2009, which deal with the blocking of websites. Under this law, the government has blocked the access to several websites. The IT rules that were adopted in 2011 require companies keeping confidential users' personal information to enforce certain defined security standards to protect data from theft.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

IV. INDIAN JURISPRUDENCE ON DATA PROTECTION AND PRIVACY

Article 21: – Article 21 of the Indian Constitution provides that 'No person shall be deprived of his or her life or personal liberty, except in accordance with the' procedure provided for by law.' However, the' right to privacy 'is not expressly recognized by the Constitution of India as a fundamental right. This question has been brought before the judiciary on many occasions and the judiciary has had different views on various cases. In the case of M, whether the right to privacy is a part of Article 21 has been raised. Ors and P. Sharma.V Satish Chandra, Magistrate for the District, Delhi and Ors. In this case, however, the Supreme Court refrained from granting the right to privacy as a basic right[8].

In the instance of R. Anr.and Rajagopal. The V State of Tamil Nadu Supreme Court observed that "the right to privacy is implicit in the right to life and liberty guaranteed by Article 21 to the citizens of that country." The "right to be let alone" is a right. A individual has the right to protect his own privacy.

"The Supreme Court subsequently stated in the case of the People's Union for Civil Liberties (PUCL) v Union of India that "we do not hesitate, therefore, to hold that the right to privacy is part of the right to "life" and "personal freedom" enshrined in Article 21 of the Constitution.

Personal Data Protection Bill 2019

The verdict in K. S. Puttaswamy (Retd.)v Union of India contributed to the Personal Data Security Bill being introduced, which is actually a draft Data Protection Act in India. The bill was presented on 11 December 2019 in the lower part of parliament. Parliament is yet to enact it, but it gives us a fair bit of insight into the advancement of data protection laws in India. This Bill aims to control the collection by government organizations and private entities incorporated in India and abroad of personal data of individuals. The collection of data is only approved if the person consents to do so, or in the event of a medical emergency, or if the State provides its people with benefits[9].

Situation in other Jurisdiction

USA: – Enacted in 2004, CalOPPA (California Online Privacy Security Act) broke the ground in the US and made it mandatory for websites to publish privacy policies outlining the collection and use of data. Starting in 2020, a new law, namely the CCPA (California Consumer Privacy Act), will be enacted. It allows businesses to warn consumers of data processing and take additional steps to protect user information.

European Union: – With GDPR, the European Union has one of the strictest data security regimes (General Data Protection Regulation). It is founded on the principle of consent, accountability, security and control of users and threatens as much as 4 percent of the annual revenue of the company[10].

V. CONCLUSION

Certainly, the current regulations issued under the IT Act are not enough for the citizens in India. With India having such a large population, it is difficult to monitor all the information produced by the people. In times of regular data breaches, India has to provide security for the protection of its citizens' personal sensitive data by enacting laws that are well protected by the threats emerging from new technologies.

It is critical that all stakeholders align their policies with data protection requirements, promote the adoption of privacy, and discuss potential consent requirements at the time of data collection for the successful implementation of the data protection regime. With the exponential rise in the way people consume and produce data around the world, data is going to become more important day by day. It will be very essential to protect citizens' data with data driving growth. Governments around the world will have to keep up with technology that is constantly evolving and update and create new legislation that protect people's confidential personal data. A concerted effort by the government and its "data-

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

conscious" people would make this world a better "data-secure" environment that is open and sensitive to new policies and laws.

REFERENCES

- [1] National Institutes Of Health, "Data Sharing Policy," *Access*, 2003.
- [2] "Toward Fairness in Data Sharing," *N. Engl. J. Med.*, 2016, doi: 10.1056/nejmp1605654.
- [3] M. D. Bergren and K. Johnson, "Data Sharing," *NASN Sch. Nurse*, 2019, doi: 10.1177/1942602X19852934.
- [4] J. B. Fisher and L. Fortmann, "Governing the data commons: Policy, practice, and the advancement of science," *Inf. Manag.*, 2010, doi: 10.1016/j.im.2010.04.001.
- [5] B. E. Bierer, M. Crosas, and H. H. Pierce, "Data Authorship as an Incentive to Data Sharing," *N. Engl. J. Med.*, 2017, doi: 10.1056/nejmsb1616595.
- [6] M. A. Yadugiri and G. Bhasker, "The Information Technology Act, 2000," in *English for Law*, 2011.
- [7] POPI, "Protection of Personal Information Act 2013," *Government Gazette*, 2013. .
- [8] O. Diggelmann and M. N. Cleis, "How the right to privacy became a human right," *Hum. Rights Law Rev.*, 2014, doi: 10.1093/hrlr/ngu014.
- [9] G. Malgieri and B. Custers, "Pricing privacy – the right to know the value of your personal data," *Comput. Law Secur. Rev.*, 2018, doi: 10.1016/j.clsr.2017.08.006.
- [10] P. M. Schwartz, "Property, privacy, and personal data," *Harvard Law Review*. 2004, doi: 10.2307/4093335.
- [11] S Balamurugan, N Divyabharathi, K Jayashruthi, M Bowiya, RP Shermy, R Shanker, "Internet of agriculture: Applying IoT to improve food and farming technology," *International Research Journal of Engineering and Technology (IRJET)*, Volume 3 issue 10, pp.713-719, e-ISSN: 2395 -0056, p-ISSN: 2395-0072, 2016
- [12] Abhishek Kumar, Bishwajeet Pandey, D M Akbar Hussain, Mohammad Atiqur Rahman, Vishal Jain and Ayoub Bahanasse, "Low Voltage Complementary Metal Oxide Semiconductor Based Energy Efficient UART Design on Spartan-6 FPGA", "2019 11th International Conference on Computational Intelligence and Communication Networks (CICN)" during 3rd - 6th January, 2019 at University of Hawaii, USA.
- [13] Abhishek Kumar, Bishwajeet Pandey, D M Akbar Hussain, Mohammad Atiqur Rahman, Vishal Jain and Ayoub Bahanasse, "Frequency Scaling and High Speed Transceiver Logic Based Low Power UART design on 45nm FPGA", "2019 11th International Conference on Computational Intelligence and Communication Networks (CICN)" during 3rd - 6th January, 2019 at University of Hawaii, USA.