DATA PROTECTION AND PRIVACY CONCERNS IN CYBERSPACE

Ms. Annapurna Trivedi[1], Dr. Upendra Nath Tiwari[2], Mr. Mridul Bhatt[3]

ABSTRACT

This paper based on doctrinal research address the emerging challenge of data protection and privacy concerns. Advancement in technology such as Mobility (Geographic Knowledge Discovery), Data Mining, Cloud computing etc. brings unforeseen challenges and one of the major challenges is threat to "privacy". Today we can access any information related to anyone from anywhere at any time but this arise a new threat to private and confidential information. Globalization has given acceptance of technology in the whole world, as per growing requirement different countries has introduced different legal framework like DPA (Data Protection Act)1998 UK, ECPA(Electronic Communications Privacy Act of 1986) USA etc. from time to time , but in India there is no such comprehensive legal framework that deals with privacy issue. To handle major cyber challenges we refer ITA Act 2008 that was built with the motivation to facilitate e-commerce and hence the privacy was not prior concern in IT act.

This paper highlights the present and future requirements of privacy laws in Indian scenario. As rightly said "true power of any law lies on its ability and ease of enforcement".

Key words: - Data privacy, organisation, Information Technology, Data protection, consumers, e-commerce, cyberspace.

INTRODUCTION

Privacy is defined as an individual's right to control his or her personal activities or intimate personal decisions without outside interference, observation and intrusion.[4] In present scenario privacy have two facets, first is privacy in the real world which can be defined as preventing a person from intrusion into one's physical space or solitude; the second is, privacy in the virtual world also known as cyber space which relates to the collection of user information from a variety of sources including the internet. Privacy in the virtual realm consists of information collection, information processing, information dissemination and invasion on private data.

With the advent of technology we have moved away from conventional modes of communication to the modern means of communication; telegram, telephone and camera are replaced by mobile phones; computer and mobile phone are readily replacing television; from reading newspapers and magazines to reading articles on internet, we have come a long way. The 21st century is also known as information age, which is associated with digital revolution.[5] Everyone and everything is interconnected and information is readily available.

Every internet user leaves a digital footprint (A trail of data a person creates while using the internet. This includes websites visited, emails sent, information submitted online) some data is collected every moment when one goes though internet, this data collection can be happening with or without the person's knowledge. Based on this, digital footprint can be divided in two categories:

1. Active digital footprint: it consists of publicly traceable information that you share on web, which includes data uploaded on Facebook, Instagram or other social media platforms or any other information, which the user posts online for public viewing.
2. Passive digital footprint: it is made up of the information that a private company reaps behind the scenes which includes IP address, purchasing history, browsing details, location data etc.

Now this digital footprint along with other data of users is often used by companies without the user's consent or knowledge to identify and predict patterns of a user's activity, this data can also be used by a private person to do some unlawful or immoral acts, for example morphing was the most prevalent cybercrime against women a few years back wherein publicly available photograph of females were changed to that of an obscene picture.

[1] Assistant Professor, ILS Shri Ramswaroop Memorial University, Dewa Road Lucknow

[2] Associate Professor, ILS Shri Ramswaroop Memorial University, Dewa Road Lucknow

[3] Student,B.Com LL.B(H), ILS Shri Ramswaroop Memorial University, Dewa Road Lucknow

[4] P*rivacy, Black's Law Dictionary* (10th ed. 2014).

[5] Castells Manuel, *The Rise of the Network Society*, Oxford, Blackwell Publishers, 2000.

DATA PROTECTION UNDER INFORMATION TECHNOLOGY ACT 2000

Under I T Act, 2000[6], few provisions are specifically provided for the purpose of data privacy in specific sense. Section 72 of the IT Act imposes liability for breach of confidentiality and privacy.

Section 43A[7] also imposes liability for breach of protection of data but limited up to the nature of sensitive personal information only. Any corporate body handling such data is responsible to protect its privacy.

This sensitive data protection rule of 2011 defines sensitive personal data or information under section 3[8] includes personal information including financial and private information of people.

Recently, a Bill to protect Data is introduced in the house named The Personal Data (Protection) Bill, 2019. The Bill does not provide any definition of privacy however; it focuses on the protection of personal and sensitive personal data of person. Bill proposes to give overriding effect on all existing provisions directly or remotely related to privacy. It proposes to prohibit that no person shall collect share, process disclose or otherwise handle any personal data of another person except in accordance with the provision of proposed Bill. The Bill proposes security to the personal data of citizens. It is pertinent to note that no privacy protection is provided to data on social media. Even the government under the scheme of Aadhar Card, collecting information of citizens without ensuring protection of security. The Bill defines the term 'Personal Data' to include Biometric data, sexual preferences, medical history and health, political affiliation, religion, race, caste, financial and credit information. This definition differs from the definition provided in the Reasonable Security Protection and Procedure and Sensitive Personal Data and Information Rule 2011. Thus the ambit of personal data has been enhanced in the Bill.

Bill also proposes certain exceptions to the violation of privacy of data on the grounds of medical emergency, national security, to prosecute for cognizable offence etc. The Bill provides that when offence is committed person will be strictly criminally liable for imprisonment and fine. It requires no assessment of intention or mens rea.

INVASION OF PRIVACY IN CYBER WORLD:

Due to the excessive dependence on the computer, as a tool for information sharing and retention of data and the use of the internet as a medium for data transfer, various invaders who indulge in the act of stealing the information, as shared through online by the user, either by use of malicious spyware, or by various computer bugs, or the data as collected from the website which is stored in the cookies folder of the computer.

Also the information that the user shares in the social networking profile i.e. LinkedIn, Twitter, Facebook, Instagram, etc. are very prone to be accessed by any intruder and are easily manipulated and misused causing privacy intrusion issues to the concerned social media user. Threats also like email attachment containing malware that discloses personal information of the recipient of the mail to the sender or any intruder. Children, who use the internet, are also easy prey of the intruders because all the information fed by a child can be easily tracked by cybercriminals.

PARLIAMENTARY REPORT ON CYBER SECURITY & RIGHT TO PRIVACY:

The Parliamentary Standing Committee on Information Technology in its 52nd Report on Cyber Security and Right to Privacy said that a significant increase in cyberspace activities and access to internet use in India coupled with lack of user end discipline, inadequate protection of computer systems, and the possibility of anonymous use of ICT allowing users to impersonate and cover their trends of crime has emboldened more number of users experimenting with ICT abuse for criminal activities. The Committee is of the opinion that this aspect has a significant impact in blunting the deterrence effect created by the legal framework in the form of the Information Technology Act, 2000, and allied laws.

The Committee has listed several offenses which fall under the purview of cyber-crimes and the remedies available within the existing legal framework. Cyberstalking or stealthily following a person and tracking his internet chats is punishable under Sec 43 and 66 of the IT Act, 2000 while video voyeurism and violation of privacy is a crime under Section 66E of the IT Act with a punishment of three years with fine. The Department of 82 Electronics and Information Technology (DeiTY) during the course of evidence submitted to the Committee that with regard to the data pertaining to privacy related cases booked under Sec 72(A) of the IT Act the number of cases registered have risen from 15 in 2010 to 46 in 2012 while the number of persons arrested were 22 in 2012.

The Committee members were of the opinion that considering the nature of cyberspace which is borderless, balancing cybersecurity, cyber-crime and the right to privacy is an extremely complex task. The members were also unhappy of the fact the government is yet to institute a legal framework on privacy. It urged upon the

[6] Information Technology Act, 2000

[7] Ibid

[8] Sensitive data protection rule of 2011

Department of Electronics and Information Technology (DeiTY) in coordination with the Department of Personnel and Training and multi-disciplinary professionals/experts to come out with a comprehensive and people-friendly policy for the protection of the privacy of its citizens[9].

COMMITTEE ON DATA PROTECTION IN INDIA, LED BY JUSTICE B.N. SRIKRISHNA,

It is said that the objective of the committee "is to ensure growth of the digital economy while keeping personal data of citizens secure and protected". The report points out several practical constraints in the implementation of many of the rights it envisages — the challenges arising from the different ways data is currently stored, the burden of meeting privacy rights, the need for exemptions, etc. For this law to be successful, recognising and addressing these constraints is important.[10]

REASONS FOR REALIZATION OF CYBER PRIVACY

According to Privacy international[11] few things have contributed to the ever-increasing privacy invasion on internet. They include:

1. Globalization, due to which geographical limitation to the flow of data is eliminated.
2. Convergence and integration is leading to the removal of technological barriers connecting systems, which is resulting in generation of easily exchangeable and interoperable information.
3. Availability of information in multimedia making it easier to translate it in other forms.

These factors make it very easy to gain access of a person's virtual data. This unlawful harvesting of data or illegal access of data is the major cause of rise in cybercrimes. According to National Crime Records Bureau's data, 11,592 cases of cybercrimes were registered in 2015, which rose to 12,317 in 2016.[12]These cases also include breach of confidentiality/privacy.

Most companies and business hire firms specializing in information processing for marketing purposes. Malicious acts like spreading malware and exploitation of bugs is also one such use of breach of privacy. Not only adults but also children and adolescents are at a greater risk as they tend to be ignorant about privacy and its implications and in turn become easy prey for private intruders. Paedophiles can exploit this vulnerability and scammers can rob a person of their money.

SUGGESTIONS

There is a need for India to constantly update the Information Technology laws so as to include the day by day increasing new threats. There is an urgent need for development and implementation of National Cyber security framework and a dedicated and specialised task force. The dimension of privacy and data protection not only needs to be considered but also needs implementation.

CONCLUSION

India does not have specific privacy legislation other than few provisions in IT Act and other piecemeal provisions of data protection. However, in absence of strong data protection law, abuse of this information can be foreseen. IT Act in India, has few provisions of data protection but has a limit to cover all the protection measures required for data security especially in transnational electronic commerce. A wide range of instances are an example to show that there are violation of data protection laws and processing of data with advent of new technology. Further the penalty imposed under IT law for violation of privacy to data by e-commerce is unable to give adequate deterrence. With the increase use of internet and people's reliance on e-commerce sites needs adequate data security regime which should provide strong rights in favour of individuals so that they can get redress against security breaches.

The Personal Data Protection Bill is heavily loaded with compliance, which may serve as a good start for regulating companies have control of user data in India. The Act also provides for penalty scheme to serve as a deterrent for non-compliance. For balancing compliance and penalties the economic and trade, interests should also be taken into consideration along with the integrity a person's virtual life. Legislation of other countries especially on the matter of cross border transfer data should be considered to make the law harmonious and interoperable. The PDP Bill is the most prominent step towards a comprehensive law on personal data protection in India.

---

[9] Report on Cyber Security & Right to Privacy submitted by the Parliamentary Standing Committee on Information Technology Act presented on Feb 12th 2014, under the chairmanship of Rao Inderjit Singh to the fifteenth of the Lok Sabha.

[10] https://indianexpress.com/article/opinion/columns/privacy-in-cyberspace-4990385/

[11] Privacy International (PI) is a registered charity based in London that works at the intersection of modern technologies and rights. https://privacyinternational.org/about (Last Visited 20th February 2021)

[12] Shaswati Das, *11,592 cases of cybercrime registered in India in 2015: NCRB,* 06 Apr 2017 https://www.livemint.com/Politics/ayV9OMPCiNs60cRD0Jv75I/11592-cases-of-cyber-crime-registered-in-India-in-2015-NCR.html (Last Visited 20th February 2021).