International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 06 | June 2021 www.irjet.net p-ISSN: 2395-0072

Privacy Issues and Data Protection Laws in Big Data as Indian Prospective

Shivam Sharma

Student, Dept. of Instrumentation Engineering, Ramrao adik institute of technology, Mumbai, Maharashtra, India

---

Abstract - India is the most densely populated economy in the world and stands second among the fastest-growing countries. India is an international hub for processing personal data. Hence, data protection laws cannot be overlooked. The Information Technology Act 2000 has some protection for personal data with improved focus on digital businesses. However, there are so many cyber crimes that still need to be focused by the Indian government. This study analyzes implications in IT Act 2000 and how PDP Bill 2019 can resolve existing data protection issues. We analyze some of the legal structures to protect credit information and private data. This paper discusses how the country is lacking individual data protection laws and a huge range of solutions. Over the past couple of years, India has made significant progress in technology. But a strict legal framework is still required for data protection.

Key Words: – data protection, IT Act 2000, Information Technology Act 2000, PDP Bill, Personal Data Protection Bill, privacy issues, data protection laws, India

1.INTRODUCTION

In 2000, the Information Technology Act was announced to boost electronic transactions and legalize e-commerce and online transactions, to promote e-governance, to ensure security protocols and practices in widespread use of information technology, improve harmonization with IT Act provisions, to prevent cyber crimes, and ensure cyber security practices for widest use of technology across the world. With the propagation of services like e-commerce, e-governance, and e-transactions related to information technology, there is a great importance of data privacy, data security, and putting security procedures into practice along with harmonization of provisions of IT Act. In addition, data security is important for economy, public safety, public health, and national security. So, it has been vital to have such infrastructure to limit and prevent unauthorized use of technology (TaxGuru, 2009).

The rapid rise in the use of internet and computer has also increased new types of crimes like transmission of phishing, offensive, and spam multimedia messages and emails, cyber terrorism, sexually explicit materials transmission through electronic media, security and privacy breaches, leakage of data, online frauds, identity theft, etc. Hence, penal provisions must be added in the IT Act, 2000. Considering the increasing cyber threats, the Information Technology (Amendment) Bill 2006 was introduced in Lok Sabha on December 15, 2006. The Bill was passed by both Lok Sabha and Rajya Sabha on December 23, 2008. On February 5, 2009, the President enacted the Information Technology (Amendment) Act, 2008 and notified the same in the Gazette of India (TaxGuru, 2009).

The Information Technology (Amendment) Act, 2008 consists of some of the important sections, viz. section 52(Allowances, Remuneration, and other Terms of Service of Members and Chairperson), section 69 (Safeguards and Protection for Monitoring, Interception, and Decryption of Data), section 54 (Provisions for Investigation of Incapacity or Misbehavior of Members or Chairperson), section 69A (Safeguards and Procedure for Blocking Information Access from public), notification as per section 70B for appointing Computer Emergency Response Team, and section 69B for safeguard for collection and monitoring of traffic data (TaxGuru, 2009).

The Personal Data Protection Bill 2019 or PDP Bill is the first data protection and data privacy regulatory bill in India. It referred both houses of the Parliament to the Joint Select Committee rather than the Standing Committee. Currently, the bill is aimed to control cross-border data transmission and ensure personal data security with the Data Protection Authority (Gupta & Tewari, 2019).

It may be the beginning in India to recognize the importance of data security and privacy. But it is still recognized among the countries with "systematic failure in keeping privacy protection" and is followed by only Russia and China with a score of 2.4 out of 5 in the international privacy index. A UK-based research firm Comparitech assessed surveillance and privacy standards in 47 countries and India is ranked among bottom five non-European countries in terms of

protecting their citizens' privacy. Other worst countries are China (with a score of 1.8) and Russia (with a score of 2.1) in protecting the privacy of citizens. Rest among the bottom five countries are Malaysia (2.6) and Thailand (2.6). The US (2.7) stands seventh among the worst performing non-EU countries.

The UK scores 3 with its official data protection act and governance of GDPR Laws. According to Comparitech, some of the major concerns of data privacy in India are a huge biometric database (Aadhar), lack of proper data protection law, and recent efforts of Indian government to make private messages on social media traceable (Gupta & Tewari, 2019). WhatsApp rolled out its revised privacy policy on January 4, 2021 for Indian users. According to this privacy policy, WhatsApp will share the messages and metadata of users with business accounts and Facebook (Khetarpal, 2021). Another interesting fact is that WhatsApp could do this only in India, not in EU countries, especially because of lack of proper data protection law (James, 2021).

The Ministry of Electronics and Information Technology, in 2019, issued the draft PDP Bill in Parliament. Currently, it is referred to the Joint Parliamentary Committee and is yet to be passed by law (Agarwal, 2020). According to PDP Bill Class 11(2)(c)[1]data principals have authority to give special consent. It is mandatory that data can be collected only for the purpose approved by the data principal, as per Clauses 5 and 6. However, WhatsApp can get away with these provisions arguing that users have already been allowed to use their metadata for messaging service and to share the same with Facebook. In its defense, WhatsApp may claim that nothing is hidden from the users (Bhushan, 2021).

The problem here is that users or data principals end up with a lack of choices. Either they can reject the terms and lose their permission to send messages through WhatsApp or allow it to use their data for other purposes. In Clause 11(3)(c), a data fiduciary is required to seek permission to process sensitive information individually for each purpose. If this provision was in practice, WhatsApp could not take consent for any of those purposes as the chats and metadata with WhatsApp business accounts that would be shared with Facebook could expose sensitive private data like sexual orientation, health data, etc. (Bhushan, 2021).

However, the privacy policy of WhatsApp would not go recognized with this data protection pressure. This update on privacy policy may also be a standard contract as users cannot negotiate the terms. They either reject them or accept them. There is no difference in a typical contract and a standard contract in the Indian Contract Act, 1872. However, there are principles from the judiciary system that should be respected. When someone is left with no choice or no other choice than signing on the contract and accepting its unfair clauses, such agreement should be deemed illegal and unreasonable[2]. Those contracts simply remove the right to choose from an individual. The recent privacy policy of WhatsApp is doing the same. There is no other choice for the users except accepting their terms or losing all the features that they were using. According to the Supreme Court (2015), forcing a party to either sign a contract with invalid and irrational terms or give up the services is grossly unfair and such contract must be void. Hence, a strict statutory and comprehensive policy is required to protect users' privacy rights. The PDP Bill strengthens consent and purpose limitations in the data protection system in India to keep track of the authority of data fiduciaries (Bhushan, 2021).

Literature Reviews

Ahmad et al. (2021) focus on information and communication technology (ICT) and its effects on security and privacy of e-health data. It is well known that there is a huge investment in ICT from medical fraternity across the world to provide better healthcare services across the world. E-healthcare systems have been used widely by medical experts with digital and multimedia technologies to improve healthcare services like application, diagnosis, and training. They discuss privacy issues in e-health security models at various phases. It is vital to have role-based access because different users access this information using e-health systems.

Right to privacy is an important fundamental right in Article 21 of the Indian constitution. While considering the urgency of framing strict rules for data privacy and protection, the Supreme Court has given its verdict on Privacy Judgment. This law was much

[1] http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

[2] https://indiankanoon.org/doc/477313/

needed to protect personal data of Indian users considering the fact that the privacy of people was at risk due to the use of data for the growing digital economy. A committee was formed on that matter to prepare a data protection framework. In December 2019, the PDP bill was drafted before the Lok Sabha. It was mostly influenced by California Consumer Protection Act (CCPA) and EU General Data Protection Regulation (GDPR). **Sen (2021)** discusses and compares important provisions of the PDP draft bill and GDPR.

According to **Mishra (2021)**, Complex data governance framework in India is addressed by several policy concerns, such as building digital startups and data champions, protecting privacy, improving government influence over data, and preventing data colonialism. The framework is largely nationalist which reinforces the antagonistic state of the country for negotiating rules about digital trade in several regional and global aspects. But the impact is still unclear on both global and digital economies and undervalued. Along with losing the opportunity to shape the rules of digital trade to promote collaboration of developing countries, India also risks the long-term economic and political interests. There is a need to balance the digital economy and national interests.

Greenleaf (2011) discusses how economic importance and size of Indian economy has led to scrutiny in privacy laws and data protection over the years. The government of India has enacted dissimilar laws regarding data protection in aspects like credit information, information technology, and access to government data. This study discusses the expansion of privacy protection through the courts. It shows that India is still lagging behind without having a comprehensive data protection framework and most parts of this law fail in protecting the rights of people. The author analyzes the basic data protection principles which are not implemented well in legal provisions of the country.

It is assumed that India has weak privacy laws in India. This assumption is still unanswered and is based on a paradigm that doesn't consider that the privacy concept is usually influenced in India with its 'culture of trust'. Researchers in the West, instead of considering specific political, social, and economic factors responsible for the controversy, have constantly varied the extent and sense of 'right to privacy' for justifying their arguments. **Basu (2010)** explains why it is not possible to enact data privacy legislation in India like the Data Protection Directive in the EU nations. The author also argues that the private domain of someone must be subjective and depends upon environment, culture, and economic condition.

Research Objectives

- To understand privacy issues in India
- To know the loopholes in IT Act 2000
- To find out how PDP Bill 2019 can solve current data protection problems

Research Questions

- What are the current loopholes in IT Act 2000 that are compromising security of Indian users' data?
- How could the PDP Bill 2019 resolve this privacy issue?

Methodology

There is still a lack of comprehensive data protection law in India except credit reporting. Data protection regulations are scattered all around the legislation. The IT Act 2000 has no limitations on the internal use of private data collected by the companies. In addition, the Right to Information Act 2005 has its limitations for access rights. There is still a lack of major protection in Indian law regarding the use of private data. In order to find the weaknesses of IT Act 2000 and whether PDP Bill 2019 has any solution, we have collected secondary data from various government reports, websites, research journals, and other authentic references to help researchers find further evidence.

Q1. What are the current loopholes in IT Act 2000 that are compromising security of Indian users' data?

The IT Act 2000 was basically enacted to legalize ecommerce in India. A lot of provisions are focused on building digital certification in the nation. Cybercrime was not added as a term in the act. It is considered with some of the cases of computer crimes. The Act defines these acts in its Chapter XI –

- Section 43 – It consists of intrusion of the virus, illegal activities, manipulating online accounts, denial of services, and causing damage.

- Section 66 - It includes the act of hacking which leads to wrongful damage or loss.
- Section 65 – Destroying, tampering, and concealing code.
- Section 67 – Acts related to transmission, publishing, or posting obscene content.

In Sections 65 and 66, there is a provision of three years of imprisonment, fine up to Rs. 2 lakh or both. There is a punishment of up to 5 years for first-time offenders in Section 67 with Rs. 1 lakh as fine. If the offense under section 67 is booked by the same person again, it will attract imprisonment for 10 years with fine up to Rs. 10 lakh (Chakraborty & Kusuman, 2014).

Problems in the Act

Though the Act has set down the framework of cyber regulations successfully and addressed some major events of misuse of the internet, there are some serious lacunae that are worth discussing. According to a cyber rights activist and Supreme Court lawyer, Pawan Duggal, the Act has not been effective to issue sanctions or penalties against offenders who misused cyberspace (Zargar, 2013). Here are some of the areas still unexplored by cyber laws in India -

Spamming – Unsolicited bulk email or spam was basically a nuisance but it is now causing serious economic issues. Strict legislation is needed to deal with spam with proper technical protection. There is no mention of 'spamming' in the IT Act. There is an anti-spam law in both the EU and the US. Australia also has strict spam legislation with a fine up to $1.1 million per day against the spammers (Chakraborty & Kusuman, 2014).

Phishing – It is a criminally fraudulent activity in which hackers attempt to get sensitive data like credit card details, username, and passwords by being masked as a trusted entity through electronic communication, such as email or website, where they make people enter financial and personal details. It is a kind of social engineering technique to manipulate users. The Information Technology Act has no strict law against phishing. Indian Penal Code has mentioned "cheating" which is not sufficient to control this activity. A phishing attack was observed when a clone of the official SBI website was used to trick the SBI customers. Even worse, there was no alert issued by the SBI. So, a legislation which restricts this activity in India is much needed (Chakraborty & Kusuman, 2014).

Identity Theft – It is an emerging cyber security problem across the world. The Information Technology Act still fails to cope with this problem. India needs companies to prevent identity theft for most of the outsourcing works (Chakraborty & Kusuman, 2014).

Internet Banking frauds – Data protection laws basically aim to protect the interest of people when someone else is processing or handling their data. Internet banking also involves several third parties along with the banks and customers. Information stored by banks about their transactions and customers is subject to changes over time. Banks cannot keep information in their own networks. There are high risks in tampering or leakage of information. It needs proper technical and legal protection. There is still a lack of data protection law that can govern a specific area for data protection in online banking. The IT Act discusses unauthorized access but there is no mention about keeping the transaction integrity. The act does not make the banks responsible to protect their clients and customers' data. A data protection law was enacted in the UK in 1998 which makes handlers of sensitive data responsible for any damages for failure in maintaining proper security of data. In India, there is no statute and banks protect customers' data out of contract (Chakraborty & Kusuman, 2014).

Q2 - How could the PDP Bill 2019 resolve this privacy issue?

Internet users have been frightened to do anything personal online without privacy. They cannot make important decisions related to online transactions and personal autonomy. The Personal Data Protection (PDP) Bill, 2019 was introduced to ensure an effective legal system in India to protect data privacy in the Lok Sabha. The PDP Bill is designed to form a special "Data Protection Authority" to protect and secure the privacy of people on the web. This bill was drafted to protect the data of people and avoid any misuse. There are also criticisms that it might cause serious misuse related to surveillance (Singh, 2020).

The central government can exempt its agencies under the bill from the provisions of IT Act for the security of public order, state, and integrity of the country, sovereignty, and friendly relationships with foreign states. The bill requires social media platforms to build a mechanism for every user in India who uses their service or registers for their service which includes a voluntary verifiable account. The provision makes the company responsible for such a mechanism. Companies will also have more responsibilities as per

the volume of data collected from the users, such as appointing data protection officials, timely audits, and data protection assessments. Social media platforms will also be responsible to verify customers' accounts (Singh, 2020).

Data protection is also based on data transfer. The Bill has been in the limelight for a lot of tech giants and Indian firms worldwide. The Bill has provisions to deal with misuse of private data in India. It makes data processing activities mandatory like data storage, protection and management. But there are some implications regarding foreign investment, international trade, and national security which should be addressed. Some people believe that it would pose new and major threats to the privacy of Indian users as the bill enables the government to access customer information. The smartphone market in India is much saturated and there are millions of internet users, which have led to a rise in digital startups. So, proper guidelines to secure private data are strongly needed with proper balance of protection and privacy of personal data (Singh, 2020).

Findings

India has recently witnessed increasing cases of cyber crime and experts blame the obsolete Information Technology Act behind it. The IT Act has failed miserably to keep track of cyber crime. The PDP Bill would have added transparency and control for the customers and helped them to own their data. Data collected from a customer should not be shared with third parties without their consent. Awareness on personal information usage, privacy, and records of processing would provide added control to the customers in terms of where, how, and why their private data is being processed. The rights of the people to access the data, correction, data portability, and objection to processing would further improve personal choice and transparency. Companies would be required to protect the IP address of the people, name, browsing history, address, and financial records.

Both government and private organizations would be held liable for the usage and processing of personal and sensitive data if PDP Bill becomes the law. It would bring more transparency about how citizens' data is handled by the government. This measure would indirectly be helpful to the government to implement further security for the protection of this type of data. The bill is applicable across the borders. The PDP bill introduced trust scores, security parameters, data audits, and other standards to make a uniform structure for data protection in India.

3. CONCLUSIONS

India is still at the beginning of having personal data protection. There are some promising signs but there is still a need to implement the most vital legislative protections. Currently, there is a strong need to have proper data protection in all sectors to meet global standards. The principles of credit reporting have most of the aspects of data protection and they can be generalized to cover different types of data. Fortunately, the awareness of cyber security measures is growing and the government is trying hard to protect the privacy of citizens. But there is still a strong need to protect Indian consumers' data with a strong law against cyber crimes.

REFERENCES

1. TaxGuru. (2009). Information Technology (Amendment) Act, 2008 Comes Into Force. Retrieved 15 May 2021, from https://taxguru.in/finance/information-technology-amendment-act-2008-comes-into-force.html
2. Gupta, M. & Tewari, S. (2019). Tipping the scale: Weighing Personal Data Protection Bill 2019 against EU's GDPR- Technology News, Firstpost. Retrieved 15 May 2021, from https://www.firstpost.com/tech/news-analysis/tipping-the-scale-weighing-personal-data-protection-bill-2019-against-eus-gdpr-7796161.html
3. Khetarpal, S. (2021). Why WhatsApp's clarification on privacy policy is misleading. BT Buzz. Retrieved 15 May 2021, from https://www.businesstoday.in/current/policy/bt-buzz-why-whatsapp-clarification-on-privacy-policy-misleading/story/427978.html
4. James, N. (2021). WhatsApp's new privacy policy: Yet another reason why India needs data protection law. Retrieved 15 May 2021, from https://www.thehindubusinessline.com/info-tech/whatsapps-new-privacy-policy-yet-another-reason-why-india-needs-data-protection-law/article33542521.ece
5. Agarwal, S. (2020). Joint parliamentary committee wants more time to submit data bill note. Retrieved

15 May 2021, from https://economictimes.indiatimes.com/tech/internet/jpc-wants-more-time-to-submit-data-bill-note/articleshow/74800912.cms?from=mdr

6. Bhushan, A. (2021). WhatsApp Privacy Controversy and India's Data Protection Bill. The Leaflet. Retrieved 15 May 2021, from https://www.theleaflet.in/whatsapp-privacy-controversy-and-indias-data-protection-bill/.
7. Ahmad, G. I., Singla, J., & Giri, K. J. (2021). Security and Privacy of E-health Data. In Multimedia Security (pp. 199-214). Springer, Singapore.
8. Sen, P. (2021). EU GDPR and Indian Data Protection Bill: A Comparative Study. Available at SSRN 3834112.
9. Mishra, N. (2021). Data Governance and Digital Trade in India: Losing Sight of the Forest for the Trees?. Forthcoming Chapter in DataSovereignty along the Digital Silk Road.
10. Greenleaf, G. (2011). Promises and illusions of data protection in Indian law. International Data Privacy Law, 1(1), 47-69.
11. Basu, S. (2010). Policy-making, technology and privacy in India. Indian JL & Tech., 6, 65.
12. Zargar, H. (2013). India's Information Technology Act has not been effective in checking cyber crime: Expert. DNA India. Retrieved 21 May 2021, from https://www.dnaindia.com/technology/report-india-s-information-technology-act-has-not-been-effective-in-checking-cyber-crime-expert-1818328
13. Chakraborty, S. and Kusuman, S. (2014). Critical Appraisal of Information Technology Act - Academike. Retrieved 22 May 2021, from https://www.lawctopus.com/academike/critical-appraisal-information-technology-act-2000/#_edn7
14. Singh, N. (2020). What Happens When Personal Data Protection Bill Becomes A Law?. Retrieved 22 May 2021, from https://thelogicalindian.com/campaign/save-our-privacy/data-protection-law-19812