Data Protection : Issues and Challenges

[1*]Mohsina Irshad

INTRODUCTION

Ours is a digital world, protecting data, such as that in a database, from destructive forces and from the unwanted actions of unauthorized users is the need of time hence data protection essentially becomes important. Data protection essentially involves the method and process of securing important information from corruption and loss.

With the advent of technology and e-commerce, the problems related to data protection are also increasing day by day. India has faced a tremendous increase in cybercrimes, data stealing etc. [2]India, being the host and the biggest platform of data outsourcing needs an effective and well formulated mechanism for dealing with these crimes.[3]India lacks a comprehensive data protection law unlike many developed countries as that of UK[4], USA[5] and Australia[6]. The Data (Privacy and Protection) Bill, 2017[7]has been proposed by the Centre but, it has not yet matured into a law.

The research paper essentially deals with all the efforts that have been taken in laying down a comprehensive data protection law and the need for having one. The paper will bring out a comparative analysis on data protection.

DATA PROTECTION : NEED

The term Data is often used in synonymous with the terms information[8]. EU's general data protection guidelines define personal data as any information relating to an identified or identifiable natural person.[9]In India *Information Technology Act, 2000*[10] does not define data however, the Protection of such data are covered under various specific provisions of the Act.[11]

2.2 Need for Data Protection

In the recent past, concerns have been raised both within the country as well as by customers abroad regarding the adequacy of data protection and privacy laws in the country.[12]A few incidents that happened in recent past have questioned the Indian data protection and privacy standards and have left the outsourcing industry embarrassed. In June 2005, *The Sun* newspaper claimed that one of its journalists bought personal details including passwords, addresses and passport data from a Delhi IT worker for £4.25 each.[13] Lack of data protection laws have left Indian BPO outfits still stagnating in the lower end of the value chain, doing work like billing, insurance claims processing and of course transcription[14].

Some of the various reasons that entail the need of having a specific legislation on data protection are: -

With the Digital India roll-out, push on digital payments, rising e-commerce penetration, and an unprecedented number of platforms and services transacting Personal Information of individuals, a stronger data protection regime is a must to foster trust in the data ecosystem.

Reasonable Security Practices and Procedure rules are not a substitute for a data protection regime. Most government departments and agencies are not body corporate, and hence beyond the remit of Section 43A compliance requirements[15].

Cross-border data flows are increasingly becoming a key determinant for claiming a country's share in the global digital trade. Countries are enacting new data protection regulations or amending existing laws, developing multilateral trade agreements concerning data flows[16].

Lack of a stringent legal framework for data protection has not only led to privacy

violations going unpunished, but it also limits the consumers' rights to claim compensation against casual and unethical data privacy violations and constrains the government's ability to impose fine and penalties[17].

The task of revising the data protection regime is vital for the progress of the country, and should be undertaken on priority. Rather than copying the European model, we should develop a regime that suits the Indian context and protects against privacy violations but does not stifle technology innovation.

3. LAWS AND LEGISLATION ON DATA PROTECTION IN INDIA.

3.1. Overview of Data Protection Laws in India

Presently, there is no specific legislation dealing with privacy and data protection India. The Supreme Court of India, has time and again recognized, privacy as an integral part of the right to life and personal liberty,[18] which is a fundamental right guaranteed to every individual under the Constitution of India. In the recent Supreme Court judgment[19], the Court held that *"Right to privacy is protected as intrinsic part of the right to life and personal liberty under Article 21 of the India Constitution and part of the freedom guaranteed by part III of the Constitution".*

Data protection in India is governed by loosely constructed provisions of the Information Technology Amended Act, 2008 under Sections 43-A and 72A of the Act[20]. The Act fails to define sensitive data, although three years later, IT Rules 2011[21] were issued defining in detail the term "sensitive data" and what it entails of.Section 43A applies only to any company and includes a firm, sole partnership or other association of individuals engaged in commercial or professional activities. Breach of data privacy has also been mentioned under the ITAA and is punishable under Section 72-A which penalizes the offender for a three-year imprisonment or a maximum fine of Rs 5 lakh.[22] There are other legislations in India that provide for data protection. *Indian Copyright Act* [23] provides that any person who knowingly makes use on a computer of an infringing copy of computer program shall be punishable for a minimum period of six months and a maximum of three years in prison and with fine which shall not be less than fifty thousand rupees but which may extend to two lakh rupees[24]. In *Burlington Home Shopping Pvt. Ltd.* v. *Rajnish Chibber* [25] the issue was whether a database consisting of compilation of mailing address of customers can be subject matter of a copyright. The Court answered the question in affirmative and held that compilation of addresses developed by anyone by devoting time, money, labour and skill amounts to a literary work wherein the author has a Copyright.Further the Indian Penal Code, punishes the dishonest misappropriation or conversion of "movable property" [26] for one's own use.

Further,*The Aadhaar (Targeted delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016* provides for specific protection of biometric data given to obtain Aadhar number by an individual. The Aadhaar Act mandates that the Unique Identification Authority of India shall ensure security and confidentiality of identity information and authentication records of individuals[27].

India is in need of a comprehensive legislation on data protection. The Data (Privacy and Protection) Bill, 2017[28] grants a statutory Right to Privacy under Section 4. Though this Bill seems to be a step in the right direction, what it can fetch is a question that remains to be answered.

4. DATA PROTECTION: A COMPARATIVE APPROACH

4.1 European Union : Protection of

people's data has been included as one of the fundamental rights of the European Union under Article 8 [29]of the Charter of the Fundamental Rights of the European.

The European Union Directive 95/46/EU[30], lays down the liability of data breach on the data controller. Self-Regulating Scheme for data privacy form an important part of the EU data protection regime.[31]The objective of this new set of rules is to give citizens back control over their personal data, and to simplify the regulatory environment for business. The data protection reform is a key enabler of the Digital Single Market which the Commission has prioritized. The reform will allow European citizens and businesses to fully benefit from the digital economy.[32]

EU superseded the Data Protection Directive with the General Data Protection Regulation in 2016 and the same Regulation will be enforceable from 2018[33]. The Regulation will be applied to all 28 of the European Union members.

4.2 Japan : After European Union, Japan introduced a separate central legislation for protection of data as the Act on the Protection of Personal Information. The Act took partial effect in 2016 and has been enforceable from May 30, 2017[34]. The law defines the scope of the legislation and states on whom the law is applicable[35].

4.3 Australia : The Australian Federal Constitution and the Constitutions of the six states and two territories does not contain any express provisions relating to privacy. However, in 2004 the Australian Capital Territory became the first jurisdiction to incorporate a bill of rights[36].

4.4 China : In China Cybersecurity Law that took effect on May 1, 2017, forbids people from using information networks to violate the privacy of others, using illegal methods to acquiring personal information, and using their positions of access to acquire, leak, sell or share personal information[37].

4.5 USA : The First Amendment of the United States Constitution guarantees the right to free speech[38]. While free speech is an explicit right guaranteed by the United States Constitution, privacy is an implicit right guaranteed by the Constitution as interpreted by the United States Supreme Court, [39]although it is often an explicit right in many state constitutions.[40]

United States has a sectoral approach [41]to data protection legislation, which relies on a combination of legislation, regulation, and self-regulation, rather thangovernmental regulation alone.Some of the federal laws in the United States which cover the law on data protection are, *The Privacy Act of 1974*[42], an extension of the *Freedom of Information Act of 1966*[43]. The Act sets forth some basic principles for disclosure of information with consent and the purpose for same to be announced in advance. *The Video Privacy Protection Act*[44] forbids a video rental or sales outlet from disclosing information concerning what tapes a person purchases. *Right to Financial Privacy Act*[45]mandates that the Federal Government present proper legal process or formal written request to inspect an individual financial record kept by a financial institution. *Federal Aviation Act*[46] directs that the information of passengers should be kept confidential. *Health Insurance Portability and Accountability Act* includes provisions such as restricting the disclosure of patient identifiable information[47].

Although there are many legislations that govern the law on data protection in US. However, it lacks a comprehensive legislation on data protection that will insure the protection of data and its secure transmission.

5. CONCLUSION AND SUGGESTIONS.

Concerns over cybersecurity, data protection and privacy have increased manifold, with the

alarming rise in incidents of breach in India and the world over the most recent case being the cyberattacks through a ransomware, WannaCry. These attacks and breaches threaten to trigger heavy damages, including loss of data and disruptions in business.

There is growing demand for India to write laws on data protection and privacy in the wake of the Supreme Court ruling on privacy to be a fundamental right. Further, with regulators like the Reserve Bank of India providing for strict privacy norms in certain areas, it seems that India is taking a huge step towards privacy norms. It is being felt by all concerned that a dedicated data protection law would give further impetus to not only the outsourcing industry but to the Foreign Direct Investment Policy at large.

SUGGESTIONS

A well-functioning data privacy regime should ideally involve transparency, consent, and accountability as its fundamental building blocks. Moreover, with technology constantly evolving, an approach based on standards would enable the law to keep pace with rapid changes in technology, as against objective rules that would fail to be relevant with constant technological developments. Further, with regulators like the Reserve Bank of India providing for strict privacy norms in certain areas, it seems that India is taking a huge step towards privacy

Perhaps the biggest shift required from the existing regime is with respect to its applicability. It is imperative to bring government agencies within the ambit of the new framework. Regulating only the collection of data may not be enough, its use by data collectors and data processors could also be regulated such that there is a prohibition on using certain data in a manner that is detrimental to data subjects.

A robust and well-functioning data privacy legislation will go a long way in complementing the constitutional right to privacy, in not only creating the right incentives for all stakeholders but also providing an efficient redress mechanism for data subjects.

(Endnotes)

1 *Mohsina Irshad BA.L.L.B (2011-2016) & L.L.M(2016-2018), NET/JRF 2017Jamia Millia Islamia

2

3 Nandan Kamath, *Law Relating to Computers, Internet and E-Commerce – A Guide to Cyberlaws* 167 (Universal Law Publishing Co., Delhi, 4thedn., 2009).

4 European Union Data Privacy Directive 1996.

5 The Privacy Act of 1974, The National Association of Service & Software Companies Act, Credit Information Companies Regulation Act, 2005, The Video Privacy Protection Act

6 Section 12 of the Australian Human Rights Act 2004.

7 Data Protection Bill 2017, *Available at:* https://www.gov.uk/government/collections/data-protection-bill-2017 (LastModified: Jan 3, 2018)

8 Verma, Ashutosh, "Data Protection Law in India: A Business Perspective", 3 *Journal of Commerce & Accounting Research* 26 (2014).

9 Regulation (Eu) 2016/679 of The European Parliament And Of The Council, Available at: http://www.livelaw.in/data-protection-india/(Last Modified: 20 Jan. 2018).

10 The Information Technology Act, 2000, Sec. 2(1)(o) defines data.

11 The Information Technology Act, 2000, Sec. 43, Sec. 65, Sec. 66, Sec. 72

12 Parag Diwan and Shammi Kapoor, Cyber and e-commerce laws, 2nd ed., [2000], p.4

13 Soutik Biswas, How secure are India's call centers, Available at http://news.bbc.co.uk/2/hi/south_asia/4619859.stm(Last Modified: Dec17, 2017).

14 Rahul Sharma, Data protection and privacy: choices before India, Jul 18 2017, Available at: http://www.livemint.com/Opinion/9NpEeZuMtxvMKZpfbD1LRN/Data-protection-and-privacy-choices-before-India.html(Last modified: Jan. 15, 2018). In the absence of data protection laws, the kind of work that would be outsourced to India in the future would be limited. The effect of this can be very well seen in the health-care BPO business, which is estimated to be worth close to $45 billion

15 Section 43A of The Information Technology Act 2008.

16 Anita Jain "*Data Protection: Security to be increased in Indian IT*",(*The Financial Times*. 24 2006)

17 Rahul Sharma, Data protection and privacy: choices

before India, *Science & Technology Law Review* 25 (2016).

18 *Kharak Singh* v. *State of U.*P AIR 1963 SC 1295; *Gobind*v. *State of M.P*. AIR 1975 SC 1375; *R. Rajagopal v. State of Tamil Nadu* (1994) 6 SCC 632; *People's Union of Civil Liberties v. Union of India* AIR 1997 SC 568; *Distt. Registrar and Collector, Hyderabad v. Canara Bank* AIR 2005 SC 186

19 *Justice K. Puttaswamy Vs. Union of India* Writ Petition (Civil) No. 494 OF 2012 (Judgment was delivered on 24.08.17)

20 Information Technology Amended Act, 2008.

21 Nikki Swartz, India to Adopt Data Privacy Rules, 37 *Information Management Journal*, 10 (2003).

22 Aparna Viswanathan, *Cyber Law,* 230 (Lexis Nexis, edn., 2nd , 2015)

23 B L Wadehra, *Law Relating to Intellectual Property*, 250 (Universal Law Publication, 5th Edition, 2012)

24 *Ibid* 253.

25 1995 PTC (15) 278 *Diljeet Titus, Advocate* v. *Alfred A. Adebare and Ors* 130 (2006) DLT 330

26 Sec. 403 of Indian Penal Code, Movable property has been defined as property which is not attached to anything and is not a land. Thus includes the Data which is a movable property.

27 Section 33, The Aadhaar (Targeted delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

28 Data Protection Bill 2017, *Available at:* https://www.gov.uk/government/collections/data-protection-bill-2017 (Last Modified: Dec,7 2017)

29 Sonakshi Awasthi , Data privacy: Where is India when it comes to legislation?, Indian Express, August 24, 2017

30 W.S. Blackmer, "GDPR: Getting Ready for the New EU General Data Protection Regulation". *Information Law Group*. InfoLawGroup (Retrieved: 2 Jan 2018).

31 Walden, *Data Protection,* 200 (London: Oxford Univeesity Press, edn., 5th, 2003).

32 Chris Reed, *Internet Law* 302 (Universal Law Publication, edn., 2nd 2010)

33 *Id.*

34 *Supra* 69.

35 Article 2 of the Act on the Protection of Personal Information (APPI).

36 http://www.privacyinternational.org/article.shtml?cmd. (Last modified: Jan 15, 2018).

37 http://www.business-standard.com/article/economy-policy/right-to-privacy-what-us-eu-china-can-teach-india-about-data-protection-117100300230_1.html (Last modified: Jan. 3, 2018).

38 Barkha and U. Ram Mohan, *Cyber Law and Crimes*, 165(Asia Law House, Hyderabad, edn., 3rd, 2016)

39 Roe v. Wade, 410 US 113 (1973)

40 Article 1 of the California Constitution: "All people are by nature free and independent and have inalienable rights. Among these are privacy."

41 Lloyd, Ian J. (2011). *Information technology law*, 26 (Oxford University Press. 6th ed. ISBN 978-0199588749)

42 Reidenberg&Gamet-Pol, The Fundamental Role of Privacy and Confidence in the Network, 30 Wake Forest Law Review 105(1995)

43 5 USC 552 a

44 8 USC 2710

45 5 USC 1693

46 49 USC 40101

47 Health & Human Services, Standards For Privacy of Individually Identifiable Health Information, 65 *Federal Register 82462-82829*, (Codified at 45 C.F.R., para 160).