DATA PROTECTION: INDIA IN THE INFORMATION AGE

Abstract

Protection of personal data requires a blend of data security with the rights conferred on the individual described by that data. While data security is an important aspect of data protection and is addressed by laws dealing with protection of electronic data storage and processing resources, other significant aspects of data protection such as an individual's right to be informed and his prior approval for data collection, processing and sharing, quality of data and remedies offered to the individual consequent to these rights are often neglected. Statutory data protection in India is not restricted to information technology laws alone. Other laws securing vital aspects of data protection exist, even if such protection is secondary to their main object. Recognizing the provisions of law assuring such rights and an analysis of the mechanisms set out for their implementation could be the first step towards optimal protection of data under the existing laws and formulating a comprehensive data protection mechanism eventually.

I Introduction

INFORMATION IS power. This is more true now, in this information age, than ever before.[1] Personal information is a valuable asset which needs to be protected against unauthorized access, use and modification as well as against flaws and unrestrained use. Protection of personal information, however, is often mistaken for the limited concept of data security. Such approach is fundamentally flawed because it fails to take into account the fact that the objective of a data protection regime is to achieve many ends besides integrity and safety of data.

Issues pertaining to privacy and security of personal data, disparities in national legislations and free flow of data across national borders in Europe were considered by the Organization for Economic Co-Operation and Development (OECD) resulting in recommendations adopted as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines),[2] one of the first attempt to develop a set of internationally recognized fair information practices.[3] The principles laid down

---

1 *Delhi Development Authority* v. *Central Information Commission*, 2010 SCC OnLine Del 2058: (2010) 170 DLT 440 (DB).

2 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980.

3 Hank Intven *et al* "Legal and Regulatory Aspects of E-Commerce and the Internet" in Ko-Yung Tung, Rudolf V. Van Puymbroeck (eds.), 1 *The World Bank Legal Review: Law and Justice for Development,* 90 (Kluwer Law International, 2003).

by the OECD and by the Council of Europe[4] serve as a benchmark for intent and methods for data protection. The instruments formulated under the auspices of both these organisations require data protection rules to regulate collection, access, quality and distribution of data. Concerns arising out to lack of ratification and implementation, as well as perceived shortcomings in the Council of Europe Convention led the European Commission to initiate work towards a European Union wide directive. The Council of Europe Convention furnished the building blocks of this directive, the European Parliament's directive 95/46/EC,[5] which in turn is set to be replaced by a European Union Regulation[6] in May, 2018.

The OECD guidelines neither refer to 'sensitive data' nor to 'automated processing' specifically and the basic principles of national application under these guidelines remain unchanged. While the scope of personal information protected or mechanism of data protection may be different among these structures, the fundamental tenets in the OECD guidelines, the Council of Europe Convention and the European Union directive remain largely the same as they draw the outlines of fair information practices.[7] Personal data should not be collected or processed unless there is a clear, informed consent of the person to whom the data pertains (the data subject), towards such declared collection and processing; something more than mere acquiescence. Data so collected should be proportionate to the purpose sought to be achieved by the person collecting, processing or retaining the data (the data controller or data processor, as the case may be). That personal data so collected should be protected against unauthorized access, misuse or tampering (data security, strictly speaking) is undisputed. The data subject should also have a right to be informed about his personal information in possession of a data controller and, in the event of any error, to seek a rectification thereof. Erroneous data will not only fail to serve the purpose for which such data was aggregated by the data

---

4 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981).

5 Directive 95/46/EC of the European Parliament and of the Council of Oct. 24, 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data.

6 Regulation (EU) 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data and Repealing Directive 95/46/EC (General Data Protection Regulation).

7 United Nations Conference on Trade and Development, *E-Commerce and Development Report* 162 (United Nations, New York and Geneva, 2004).

controller, it may in fact lead to severe complications for the data subject. In the United Kingdom, a person was not only refused loan repeatedly but also detained at the airport having been identified as a part of Saddam Hussein's regime. This was found to be a consequence of reliance placed on erroneous database by the banks as well as law enforcement agencies, resulting in a fraud warning.[8] In addition to such hardships to a data subject, breaches in data protection hurt businesses in a monetary sense. In 2003, a Pricewaterhouse Coopers study was reported to have found poor data management, costing businesses nearly US$ 1.4 billion a year in billing, accounting and inventory errors.[9] A 2015 study[10] found breach of data security costs at Rs.3,396 per compromised record, translating into loss of business worth Rs.21.78 million in India. In addition to the direct costs to the data subjects and controllers, the European Union directive expressly forbids onward transfer of personal data by a data controller from an EU member state to a non-member state, unless the national laws applicable to such a transferee provide an adequate level of protection to personal data, comparable to that assured under the data protection directive (the adequacy test).[11] Data protection, in this sense, assures rights far greater than what are delivered under dedicated information technology laws, as reflected in the OECD guidelines which prescribe the following eight basic principles:[12]

1. Collection limitation principle: There should be limits to the collection of personal data. Any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data quality principle: Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

---

8 M. R. McGuire, *Technology, Crime, and Justice: The Question Concerning Technomia Technology, Crime and Justice* 100 (Routledge, 2012).

9 Jack E. Olson, *Data Quality: The Accuracy Dimension* 9 (Morgan Kaufmann, 2003).

10 2015 Cost of Data Breach Study: India (Ponemon Institute, May 2015) *available at* http://www.cisoplatform.com/profiles/blogs/ponemon-report-cost-of-data-breach-in-india-2015 (last visited on Jan. 11, 2017).

11 Directive 95/46/EC, ch. IV: Transfer of Personal Data to Third Countries, art. 25(1): The Member States shall provide that the transfer to a third country of personal data … may take place only if … the third country in question ensures an adequate level of protection

12 Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 13-16 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, 2001).

3. Purpose specification principle: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use limitation principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with purpose specification principle except:

a) with the consent of the data subject; or

b) by the authority of law.

5. Security safeguards principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

6. Openness principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual participation principle: An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him:

   i) within a reasonable time;

   ii) at a charge, if any, that is not excessive;

   iii) in a reasonable manner; and

   iv) in a form that is readily intelligible to him;

c) to be given reasons if such a request is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. Accountability principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.

In 2009, the Ministry of Home Affairs, Government of India announced a project[13] proposing to integrate twenty-one categories of databases and create a unified National Intelligence Grid (NATGRID). By August, 2016, Government of India had emphasized on the application of big data analytics[14] and artificial intelligence to such a database.[15] The existence of such massive and sensitive databank makes it vital to spell out steps for protection of this data from inaccuracies as also from unauthorized access. The essential features for protection of personal data can be found in many statutes in India as diverse as the Information Technology Act, 2000, the Credit Information Companies (Regulation) Act, 2005, the Right to Information Act, 2005 and the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016. There exists a school of thought which asserts that a right in personal information ought to be treated as a property right of the individual whom the personal data relates to and protected as such.[16] That perspective, however, merits an extensive treatment of its own and this paper shall instead refer of some of the relatively established norms which may be applied for protection of personal data.[17]

II Information Technology Act, 2000: Protecting electronic data

The stated objective of the Information Technology Act, 2000 is regulation and facilitation of electronic data interchange in the course of electronic commerce. To that end, section 43 of the Act enumerates a wide range of acts with respect to computers and computer resources, which are liable to attract sanctions under the Act. These include accessing a computer without the

---

13 Press Release dated Sep. 14, 2009 *available at* http://www.pib.nic.in/release/release.asp?relid=52610 (last visited on Nov. 25, 2016); Press Release dated Mar. 1, 2016 *available at* http://pib.nic.in/newsite/PrintRelease.aspx?relid=137128 (last visited on Nov. 25, 2016).

14 "Big Data is often described as extremely large data sets that have grown beyond the ability to manage and analyze them with traditional data processing tools. … all of these data have intrinsic value that can be extrapolated using analytics, algorithms, and other techniques." Frank Ohlhorst, *Big Data Analytics: Turning Big Data into Big Money* 1,2 (John Wiley & Sons, 2013).

15 Press Release from Press Information Bureau, Government of India, Ministry of Home Affairs Aug. 31, 2016, *available at*: http://pib.nic.in/newsite/PrintRelease.aspx?relid=149414 (last visited on Nov.25,2016)..

16 Hal R. Varian, "Economic Aspects of Personal Privacy" in William H. Lehr and Lorenzo Maria Pupillo (eds.), *Internet Policy and Economics: Challenges and Perspectives* 105 (Springer, 2002).

17 See Atul Singh, "Protecting Personal Data as a Property Right" 2 *ILI Law Review* 123-39 (Winter Issue, 2016).

permission of its owner, replicating information, introducing a computer virus, damaging any database, disrupting a computer, denying access to a computer and destroying and deleting or altering information contained in a computer. Though heading to section 43 describes it as 'penalty for damage to computer', the provisions also specify unauthorized access *simpliciter*, without relating to any damage. That, in theory at least, rules out the kind of interpretative dilemma faced by the United States District Court in *Cohen* v. *Gulfstream Training Academy*,[18] for instance, where mere copying of data precluded damages for the reason of there being no interruption of service as contemplated under the Computer Fraud and Abuse Act. Under section 43A, a body corporate negligent in implementing and maintaining reasonable security practices and thereby causing wrongful loss or wrongful gain to any person is liable to pay damages by way of compensation to the person so affected. In *Poona Auto Ancillaries Pvt. Ltd.* v. *Punjab National Bank,*[19] for instance, an amount of Rs.80.10 lakh was transferred from the account of the complainant to a third-party, without his authorization. Upon investigation, none of the ultimate transferees could be located and it was discovered that the information provided by these final transferees to the respondent bank was falsified. The adjudicating officer held that the respondent bank had been negligent in following security practices and directed the bank to pay damages to the tune of Rs.45 lakh to the complainant.[20]

Data controllers and data processors execute service agreements to facilitate sharing of data and to set out the rights, duties and obligations of the respective parties. Such agreements incorporate clauses for data protection as well. When it comes to the enforcement of such right by a data subject, the fact that a data subject is neither a party to the said contract nor a beneficiary under a trust[21] may limit the contractual remedies available to such data subject. The Information Technology Act, however, through section 72A makes it punishable to disclose, without the consent of a data subject or in breach of a lawful contract, personal information accessed by a service provider while providing services under the terms of the contract.

---

18 249 F.R.D. 385 (S.D. Fla., 2008).

19 Unreported, Complaint No.4/2011, Adjudicating Officer, Government of Maharashtra, Nov. 9, 2011, *available at*: https://it.maharashtra.gov.in/Site/Upload/ACT/DIT_Adjudication_PoonaAuto_Vs_PNB-22022013.PDF (last visited on Jan. 5, 2017).

20 Contributory negligence was attributed to the complainant and he was denied any damages towards loss of interest.

21 *M.C. Chacko* v. *State Bank of Travancore*, 1970 SCR (1) 658.

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, made under section 87(2) read with section 43A of the Information Technology Act spell out a much wider protection to personal data. These rules cater to some of the most fundamental requirements of data protection: consent, notice, collection limitation, use limitation, rectification and onward transfer. Rule 3[22] includes password, financial information, physical, physiological and mental health condition, sexual orientation, medical records and history, and biometrics within the meaning of sensitive personal data. Techniques for measuring and analysing fingerprints, eye retinas and irises, voice patterns, facial patterns, hand measurements and DNA are included under the term 'biometrics'. Under rule 4, a body corporate is required to state its policy for handling personal information giving clear information about type of sensitive personal data collected, the purpose of collection and usage and security practices. Rule 5 requires consent for and proportionality of data collection and a body corporate is required not to collect sensitive personal data, unless it is required for lawful purpose connected with such corporate's functions. The information is not to be retained for a period longer than necessary for performing lawful functions and it shall be used only for such purposes (thereby creating use limitation and confining data retention). Rule 5(6) permits a data subject to review and seek correction in his personal data in possession of the data controller (individual participation). Disclosure of personal data to a third-party requires prior permission of the data subject under rule 6. Rule 7 permits transfer of personal information to a third-party which provides adequate data protection as envisaged under the rules ('adequacy', though not defined as such in the rules). In terms of rule 4, a body corporate is required to publish its privacy policy on its websites. Upon accessing the websites of Bharti Airtel Ltd.,[23] Vodafone India Ltd.,[24] Bharat Sanchar Nigam Ltd. (BSNL)[25] and Mahanagar Telephone Ltd. (MTNL),[26] the private sector service providers were found to have an easily available privacy policy setting out the information as prescribed under the

---

22 The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, rule 3 (Sensitive personal data or information).

23 *Available at*: http://www.airtel.in/forme/privacy-policy (last visited on Jan. 10, 2017).

24 *Available at:* http://www.vodafone.in/privacy-policy?section=consumer (last visited on Jan. 10, 2017).

25 *Available at:* http://www.bsnl.in/opencms/bsnl/BSNL/about_us/site_map.html (last visited on Jan. 10, 2017).

26 *Available at* :http://mtnldelhi.in(last visited on Jan. 10, 2017).

rules. So far as state owned BSNL and MTNL were concerned, no statement on their privacy policy was available on their websites, which indicates the lackadaisical approach of service providers towards data protection and raises questions on the enforcement of the principles.

III Right to information: Complementing data protection through subject access

When it comes to 'subject access', *i.e.* the right of a data subject to know about his data in possession of a data controller, the Right to Information Act, 2005 has some measures so far as data in possession of a public authority is concerned. Both specialized data protection laws and freedom of information laws provide an individual a right to know the nature and extent of information about him being stored by an organization. This aspect of freedom of information becomes all the more significant n India which does not have a special data protection law, but where the Right to Information Act forwards this aim of data protection laws. In *Manohar Singh* v. *National Thermal Power Corporation Ltd.*,[27] the central information commission had decided that when a citizen seeks information about himself and as long as the information sought is not exempt in terms of other provisions of section 8 of the Right to Information Act, section 8(1)(j) of the Act cannot be applied to deny information. Relying on the fact that 'information', as defined in section 2(f) of the Act included information relating to any private body which can be accessed by a public authority, the central information commission extended the right to information from a private hospital. In *Prabhat Kumar* v. *Directorate of Health Services, Government of NCT of Delhi*, the central information commission accordingly directed the Government of NCT of Delhi to compel a private hospital to provide the medical records applied for by the information seeker.[28]

IV Financial information

Financial information is perhaps one of the oldest forms of personal data collected and processed for commercial purposes. A credit information company primarily collects, processes and disseminates credit information. The Credit Information Bureau (India) Ltd. was such a corporation set up by the State Bank of India in association with HDFC bank in January, 2001. To

---

27 2006 SCC OnLine CIC 684, Appeal No.80/ICPB/2006, Central Information Commission, Aug. 28, 2006.

28 2015 SCC OnLine CIC 2742, Appeal No.CIC/SA/A/2014/000004, Central Information Commission, Sep. 3, 2014.

regulate such companies, the legislature enacted the Credit Information Companies (Regulation) Act, 2005. Since this enactment, no company is permitted to commence or carry on business of credit information without obtaining a certificate of registration from the Reserve Bank of India. Section 2(d) of this Act defines 'credit information', which includes amounts and the nature of loans or advances, amounts outstanding under credit cards, creditworthiness and other such aspects of a borrower of a credit institution. The extremely sensitive nature of data being collected and processed by the credit information companies raises strong concerns about its accuracy, security and privacy. Section 17(4) of the Act protects such information from unauthorised disclosure. Section 17(4)(a) requires that a credit information company shall not disclose information to any person other than a 'specified user'.[29] Section 17(4)(b) imposes similar obligation on the specified user not to disclose the credit information to any other person. Section 20 mandates credit information company to adopt privacy principles in relation to collection, processing, collating, recording, preservation, secrecy, sharing and usage of credit information. Section 21 relates to individual participation. Section 21(1) addresses the principle of access to a person to his own personal information. It provides that any person, who applies for a credit facility from any credit institution, may require such credit institution to furnish him a copy of the credit information obtained by such institution from the credit information company. Further, section 21(3) provides that if the information is not updated, the borrower may request the credit information company, the credit institution or the specified user, as the case may be, to update the information by making appropriate correction. Section 22 proscribes unauthorised access to credit information and provides that any person obtaining unauthorised access to credit information shall be punishable with fine which may extend to one lakh rupees; significantly, such unauthorised credit information shall not be taken into account for any purpose. Chapter VI of the Credit Information Companies Regulations, 2006 lays down comprehensive rules to maintain accuracy of data, access to, and modification of, data, preservation of data, *etc.* Regulation 10(a) is titled as 'care in collection of credit information'. Regulation 10(a)(i) requires a credit information company to take precautions to ensure that the information

---

29 The Credit Information Companies (Regulation) Act, 2005, s. 2(l): "specified user" means any credit institution, credit information company being a member under sub-section (3) of Section 15, and includes such other person or institution as may be specified by regulations made, from time to time, by the Reserve Bank for the purpose of obtaining credit information from a credit information company.

received or collected by it is properly and accurately recorded, collated and processed. Regulation 10(a)(ii) requires a credit information company to update the data maintained by it on a monthly basis and to take steps to ensure that the credit information furnished by it is revised, accurate and complete. Regulation 10(b) allows any person to know his own credit information from a credit information company. It requires every credit information company to disclose the credit information about a person, on his request. Protection of personal financial data is not novel to Credit Information Companies (Regulation) Act, 2005. The Reserve Bank of India Act, 1934,[30] the State Financial Corporations Act, 1951,[31] the State Bank of India Act, 1955,[32] the Deposit Insurance and Credit Guarantee Corporation Act, 1961,[33] and the Banking Companies (Acquisition and Transfer of Undertakings) Act, 1970[34] among others, direct maintenance of confidentiality of financial information. Section 45E of the Reserve Bank of India Act, 1934, for instance, provides for confidentiality of the credit information obtained by the Reserve Bank of India from any banking company; provisions in other above mentioned statutes are almost identically worded. What is unique, though, is that the Credit Information Companies (Regulation) Act deals with activities which are dedicated towards data collection and processing; such data collection and processing and thereby, data protection, is not incidental to the primary objective of the Act but is inherent to it. More importantly, and not seen in other banking laws, the Credit Information Companies (Regulation) Act provides for participation of the data subject in data processing by enabling the data subject to seek revision or correction of his personal data in possession and control of a credit information company.[35]

---

30 The Reserve Bank of India Act, 1934, s. 45E (Disclosure of information prohibited).

31 The State Financial Corporations Act, 1951, s. 40 (Declaration of fidelity and secrecy).

32 The State Bank of India Act, 1955, s. 44 (Obligation as to fidelity and secrecy).

33 The Deposit Insurance and Credit Guarantee Corporation Act, 1961,s. 39 (Declaration of fidelity and secrecy).

34 The Banking Companies (Acquisition and Transfer of Undertakings) Act, 1970, s. 13 (Obligations as to fidelity and secrecy); Banking Companies (Acquisition and Transfer of Undertakings) Act, 1980, s. 13 (Obligations as to fidelity and secrecy).

35 The Credit Information Companies (Regulation) Act, 2005, s. 21 (Alteration of credit information files and credit reports).

V Consumer Protection Act, 1986: Mechanism for enforcing personal data rights?

While financial information may be the established form of personal data, modern telecommunication service sector is a rich, relatively untapped and undemanding source of personal data. Personal information such as an innocuous phone number may potentially be associated with a unique name, age, gender, financial status and physical location of a natural person. Under section 67C of the Information Technology Act, 2000, an intermediary may be required to preserve and retain such personal information. In terms of the license agreement executed between the Government of India and the cellular mobile telephone service providers, the service providers are required to preserve billing and accounting records for a period of three years and commercial records with regard to the communications exchanged for a period of one year.[36] The nature of data collected and retained by telecom service providers and, as a consequence, associated with a unique mobile phone number, may be gauged from the privacy policies acknowledged by two major private telecom service providers in India–demographics,[37] name, address and location.[38] Can negligence in maintaining confidentiality of data so collected or the use of such personal data for a purpose not directly related to telecommunications services be considered a deficiency in service? A fault, imperfection, shortcoming or inadequacy in the quality, nature and manner of performance may amount to a deficiency in service. Service would refer to the telecommunication service and its quality and, therefore, while issues related to telecommunication connectivity must qualify as a fault and shortcoming in service, the same may not be readily extended to usage of personal information obtained in the course of providing such service. The usage of personal data may, however, be within the scope of manner of performance of service insofar as the telecom service providers undertake to maintain data protection as a part of their privacy policy (privacy policy, to that extent may even be read as terms of contract between the data subject and the data controller).

---

36 Preservation of Telecom Records, Ministry of Communications & Information Technology, Government of India Aug. 26, 2010, *available at* : http://pib.nic.in/newsite/PrintRelease.aspx?relid=65325 (last visited on Nov. 15, 2016).

37 Bharti Airtel Ltd, *available at* : http://www.airtel.in/forme/privacy-policy ((last visited on Nov. 15, 2016).

38 Vodafone India Ltd., *available at*: http://www.vodafone.in/privacy-policy?section=consumer (last visited on Nov. 15, 2016).

Despite having one of the most robust mechanisms for consumers to enforce claims arising from breach of contracts or torts, the Consumer Protection Act, 1986, has not been applied with much success to aspects of data protection. It may not be an overstatement to say that one of the early grievances raised under the Consumer Protection Act in the context of personal data was witness to an intensely contested dispute and, to some extent, judicial misadventure. In *Nivedita Sharma* v. *Bharti Tele Ventures*,[39] the complainant was aggrieved by unsolicited calls being made to her by the banks and the financial institutions marketing their services. A complaint was preferred against telecom service provider Bharti Tele Ventures and the banks, ICICI Bank Ltd. and American Express Bank Ltd. The Delhi State Consumer Disputes Redressal Commission arrived at a conclusion that these banks had obtained information regarding the telephone number, financial standing *etc.* pertaining to the complainant, from the telecom provider without authorization and without the complainant's knowledge or consent. It was held that whenever confidential information of a subscriber or consumer was traded or furnished without the knowledge or consent of the consumer, both the service provider as well as the person who procures this information are guilty of the offence of deficiency in service and unfair trade practice. The commission imposed a penalty of Rs.50 lakhs, jointly on the banks and the telecom providers and a penalty of Rs.25 lakhs to be shared between the banks. An amount of Rs.50,000/- was awarded as compensation payable to the complainant. Taking a step further, the commission passed a general order to the effect that every consumer suffering from such a nuisance shall be entitled to a minimum compensation of Rs.25,000/- as and when such a consumer approached the commission. This order of the state commission was challenged before the high court of Delhi in *Cellular Operators Association of India* v. *Nivedita Sharma*.[40] So far as punitive damage amounting to Rs.75 lakh was concerned, the high court observed that a state commission had no power to impose penalty except as provided under section 27 of the Consumer Protection Act. Even otherwise, the high court observed that the commission directed a deposit of punitive damages to a 'state consumer welfare fund', though no such fund existed. The order towards penalties was held as beyond the jurisdiction of the commission and set aside. Similarly, the directions of the commission regarding award of a minimum compensation of Rs.25,000 to every consumer was held to amount to legislation and beyond the powers conferred upon the commission under the Act. The

---

39 2007 (1) CPJ 186.

40 (2010) 166 DLT 558 : (2010) 115 DRJ 236.

dispute continued and the judgment of the High Court of Delhi was challenged by way of a petition for special leave to appeal before the Supreme Court in *Nivedita Sharma* v. *Cellular Operators Association of India*,[41] wherein the decision of the high court was set aside, granting liberty to the service providers (*i.e.* the data controllers) to approach the National Consumer Disputes Redressal Commission. Ultimately, after traversing two constitutional courts and a state commission, in *Cellular Operators Association of India* v. *Nivedita Sharma*,[42] the national commission set aside the order of state commission insofar as the compensation of Rs.50,000/- was concerned. The national commission, however, chose not to disturb the order of the state commission whereby the telecom service providers and the banks were directed to deposit a sum of Rs.75 lakh in favour of 'state consumer welfare fund'. The sweeping directions passed by the state commission (*inter alia* that every consumer suffering from such a nuisance was entitled to a minimum compensation of Rs.25,000) were directed to be treated as recommendations rather than directions. While it remains an open question whether collection, processing or sharing of personal data constitutes imperfection in the manner of performance of a service, subsequent to *Nivedita Sharma*, no significant litigation has come up under the Act.

VI Creation of personal information, protection and ID divide

One of the most recent legislative actions having direct implications on personal data in India is the enactment of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (the Aadhaar Act).[43] This Act intends to regulate delivery of subsidies, benefits and services, the cost towards which is incurred from the consolidated fund of India. Such

---

41 (2011) 14 SCC 337.

42 IV (2013) CPJ 265 (NC) : 2013 SCC OnLine NCDRC 932.

43 Before this enactment, the Government of India had propounded a "Aadhaar Card Scheme"` through which it was collecting and compiling demographic as well as biometric data of all the residents in India for use for various purposes by issuing 12-digit unique identification number. The constitutional validity of the scheme was challenged *inter alia* on the ground that it violated the 'right to privacy' guaranteed under art. 21 of the Constitution of India. The Supreme Court initially directed that "no person should suffer for not getting the Aadhaar card in spite of the fact that some authority had issued a circular making it mandatory and when any person applies to get the Aadhaar card voluntarily, it may be checked whether that person is entitled for it under the law and it should not be given to any illegal immigrant." *K.S. Puttaswamy* v. *Union of India* (2014) 6 SCC 433. Later on, while referring the matter to a larger bench, the Supreme Court passed the following directions: " Having considered the matter, we are of the view that the balance of interest would be best served, till the matter is finally decided by a larger Bench if the Union of India or the UIDA proceed in the following manner:-

regulation is to be achieved through unique identity number assigned to the individuals residing in India (Aadhaar number). The Act defines 'identity information'[44] as being composed of an individual's Aadhaar number, his biometric information and his demographic information. Demographic information[45] includes information relating to the name, date of birth, address and other relevant information of an individual; information which may be collectively termed as 'attributed identifiers', being assigned to an individual after his birth.[46] Biometric information refers to photograph, fingerprint, iris scan or other such specified biological attributes; of these, fingerprint and iris form a separate class of data referred to as the 'core biometric information'.[47] Biometric and demographic information may be collected by enrolling agencies for the purpose of issuing an Aadhaar number. The Aadhaar Act provides for

---

1. The Union of India shall give wide publicity in the electronic and print media including radio and television networks that it is not mandatory for a citizen to obtain an Aadhaar card;

2. The production of an Aadhaar card will not be condition for obtaining any benefits otherwise due to a citizen;

3. The Unique Identification Number or the Aadhaar card will not be used by the respondents for any purpose other than the PDS Scheme and in particular for the purpose of distribution of foodgrains, etc. and cooking fuel, such as kerosene. The Aadhaar card may also be used for the purpose of the LPG Distribution Scheme;

4. The information about an individual obtained by the Unique Identification Authority of India while issuing an Aadhaar card shall not be used for any other purpose, save as above, except as may be directed by a Court for the purpose of criminal investigation.":

K.S. Puttaswamy v. *Union of India*, AIR 2015 SC 3081 at 3086. After the enforcement of the Aadhaar Act, several writ petitions were filed challenging its constitutional validity. Subsequently, a five-judge bench of the court passed detailed orders on Aug. 11, 2015 as modified on Oct. 15, 2015 to the effect that the Aadhaar card scheme was purely voluntary and it could not be made mandatory till the matter was finally decided by the court. Moreover, the Aadhaar card scheme was to apply for the present for the P.D.S. scheme and the L.P.G. distribution scheme, the schemes like the Mahatma Gandhi National Rural Employment Guarantee Scheme (MGNREGS), national social assistance programme(old age pensions, widow pensions, disability pensions) Prime Minister's jandhanyojana (PMJDY) and employees' provident fund organization (EPFO). *K.S. Puttaswamy* v. *Union of India* (2015) 8 SCC 735 and (2015) 10 SCC 92. The final decision of the five-judge bench is awaited.

44 The Aadhaar Act, s. 2(l).

45 *Id.*, s. 2(k).

46 Natasha Semmens, "Identity theft and fraud" in Fiona Brookman*et al.* (eds.), *Handbook on Crime* 176 (Willan, 2010).

47 The Aadhaar Act, s. 2(g).

collection limitation insofar as it excludes race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history from the scope of demographic information. Collection limitation, consent and notice are also provided under section 3(2) which requires the enrolling agency to inform the data subject about the manner of use of the information, entities with whom information is intended to be shared during authentication and about subject access to the information. Section 28 requires the authority to ensure confidentiality of the identity information and to ensure that it is secured against access, use or disclosure not permitted under the Act, and against accidental or intentional destruction, loss or damage. Use of identity information collected under the Act, for a purpose other than the one informed to the data subject at the time of data collection, is restricted under section 29(3)(a). Onward disclosure of identity information without the prior consent of the data subject is also barred under section 29(3)(b). All types of biometric information specified under the Act is deemed[48] to be 'sensitive personal data' as set out in section 43A of the Information Technology Act which is in turn relatable to the class of information categorised as sensitive personal information in terms of rules thereunder.[49] The relatively wider set of data protection norms under the Sensitive Personal Data Rules, 2011 will, therefore, extend to the biometric information collected under the Aadhaar Act as well.

Within biometric information itself, the core biometric information is further subject to use limitation as section 29(1) which prohibits both sharing of core biometric information for any reason whatsoever and also, its use for any purpose other than generation of an Aadhaar number. So far as individual participation is concerned, section 31 of the Act enables correction of demographics information or alteration in the biometric record of an Aadhaar number holder and section 32 entitles every Aadhaar number holder to obtain his authentication record. Chapter VII lays down penalties for actions such as disclosure of information, unauthorised access, copying of or damaging data or disrupting access or tampering information. The significance of notice and consent provisions under the Act can be assessed from the fact that failure to intimate the data subject as required under section 3(2) and section 8(3) is liable to attract imprisonment which may extend to one year or with a

---

48 *Id*., s. 30.

49 The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information) Rules, 2011, rule 3 (Sensitive personal data or information).

fine which may extend to Rs.10,000 (Rs.1 lakh in the case of a company) or with both.[50]

A consequence of 'creation' of unique personal data for identification purposes has been described as an 'ID divide'[51] a segregation of individuals in possession of valid identification data and those lacking it; the latter rendered virtually incapable of undertaking seemingly commonplace everyday tasks such as boarding a plane, cashing a cheque, opening a bank account, starting a job or even exercising constitutional rights like voting in elections. In *Crawford et al* v. *Marion County Election Board*,[52] the Supreme Court of United States upheld the constitutional validity of a law[53] which required citizens voting in person to present a photo identification issued by the government, such as a driving license. Voicing his dissenting opinion therein, Sauter J observed that poor, old and disabled voters, who do not drive a car, might find it prohibitive to obtain a driving license. Multiple identity documents have perhaps only added to the ID divide in India.[54] Interestingly, the Aadhaar Act has attempted to answer just such a predicament through section 5 of the Act. Under section 5, the Unique Identification Authority of India (the Authority/UIDAI)) is required to take special measures to issue Aadhaar number to women, children, senior citizens, persons with disability, unskilled and unorganised workers, nomadic tribes or to such other persons who do not have any permanent dwelling house. Considering that personal information such as name, date of birth, residence, photograph and fingerprints[55] have been collected and retained since a long time in course

---

50 The Aadhaar Act, s. 41.

51 "(T)he ID Divide - Americans who lack official identification, suffer from identity theft, are improperly placed on watch lists, or otherwise face burdens when asked for identification…those on the wrong side of the ID Divide are finding themselves squeezed out of many parts of daily life, including finding a job, opening a bank account, flying on an airplane, and even exercising the right to vote." Peter P. Swire and Cassandra Q. Butts, "The ID Divide: Addressing the Challenges of Identification and Authentication in American Society", 3(1) *Advance, American Constitution Society for Law and Policy* 95 (2009).

52 *Crawford, et al* v. *Marion County Election Board, et al*, 553 US 181 (2008).

53 The Senate Enrolled Act No. 483: An Act to amend the Indiana Code concerning elections, State of Indiana, United States of America (also known as the 'Voter ID Law').

54 Soutik Biswas, "Bridging India's identity divide with a number" *BBC News*, May 28, 2012, *available at* : http://www.bbc.com/news/world-asia-india-18141584 (last visited on Oct. 30,2016) ; "The Great Indian Identity Crisis", *The Times of India,* Feb. 17, 2013.

55 Neha Shukla, "RTO to take fingerprints for smart driving licence" *The Times of India (Lucknowedn.)*, Jun. 10, 2009, *available at* http://timesofindia.indiatimes.com/city/lucknow/RTO-to-take-fingerprints-for-smart-driving-licence/articleshow/4637744.cms (last visited on Oct. 30, 2016).

of issuance of a driving license, without any particular data protection guidelines, it is indeed an advance that this Act clearly specifies data protection standards applicable to data collected and processed thereunder.

VII Aadhaar challenge to data protection

The Aadhaar Act attempts to satisfy some of the basic data protection requirements, providing for collection limitation, purpose specification, use limitation, security safeguards and individual participation. A closer analysis would, however, reveal the deficiencies in the Act, some of them quite substantial. Disclosure of information may be permitted in derogation of confidentiality measures[56] pursuant to an order of a court. However, an opportunity of being heard prior to such disclosure is required to be given not to the data subject but to the UIDAI.[57] Section 48 of the Act empowers the Central Government to supersede the authority in the event *inter alia* of a public emergency.[58] It is pertinent to note that the Act imposes another very significant constraint on the rights of a data subject insofar as no complaint under the Act is maintainable before any court at the instance of the data subject.[59] The law needs to introduce means for redressing the grievances of data subjects and also means for restitution to data subjects who suffer loss or harm from breach of data protection.

The collection and use of personal data under the Aadhaar Act, towards public services, is not perhaps the leading cause of concern insofar as the Act has inbuilt measures to deal with collection and processing of personal data.

---

56 As contained in ss. 28(2) and 28(5) and sharing limitation placed under s. 29(2) of the Aadhaar Act.

57 The Aadhaar, s. 33(1).

58 Neither the Aadhaar Act nor the General Clauses Act, 1897 defines a 'public emergency'. While the Indian Telegraph Act, 1885 permits taking possession of licensed telegraphs, the Indian Post Office Act, 1898 permits interception of postal article, the Noise Pollution (Regulation and Control) Rules, 2000 permit the use of a loud speaker, the Industrial Disputes Act, 1947, permits declaration of any industry as a 'public utility' in the event of a public emergency, no motive is discernible in superseding the unique identification authority so far as the purposes of Aadhaar Act are concerned, more so since s. 33 of the Act itself moderates the application of non-disclosure provisions in the interest of national security, without any need of a concomitant public emergency.

59 The Aadhaar Act, s. 47. (1): No court shall take cognizance of any offence punishable under this Act, save on a complaint made by the Authority or any officer or person authorised by it, Aadhaar Act.

Even if such measures are criticized as rudimentary, the basic principles of data protection are recognized under the Act and are always amenable to 'restatement'. Some of the concerns of data protection are not really inherent deficiencies to Aadhaar itself, but rather, to a creation of inter-linked databanks with Aadhaar as its nucleus. If a citizen's Aadhaar details, financial data and taxation records are interlinked, all of them are accessible only with the knowledge of the person's unique Aadhaar number. And, whereas the personal data collected under the ambit of Aadhaar Act itself is offered some protection under the Act, the information collected under other laws, but ultimately linked to Aadhaar number, do not get the same level of protection. The nature and amount of data available to NATGRID,[60] for instance, which is set up not under the Aadhaar Act but under a notification of the Government of India[61] and, thus, not subject to any statutory limitations, is particularly ominous. According to news reports from April, 2017, it has been stated on behalf of the Government of India, that the Aadhaar number shall not be linked with the NATGRID.[62] The reason forwarded in support though, makes this assertion sound less reassuring. The Minister of Law and Justice and Information Technology is reported to have stated that according to section 29(1) of Aadhaar Act, biometrics could not be disclosed to anyone. This fails to take into account the fact that in terms of section 29(1), whereas core biometrics cannot be shared, identity information, other than core biometrics, can be shared in accordance with the provisions of the Act. Section 29 does not provide checks on use of non-biometric identity information such as demographics for national security.

What is, however, most alarming is a seemingly *laissez faire* unregulated access to personal data offered to private entities. In terms of section 8(1) of the Act, the authority shall perform authentication of the Aadhaar number of

---

60 National Intelligence Grid.

61 "National Intelligence Grid (NATGRID) has been set up as an attached Office of the Ministry of Home Affairs with effect from Dec. 1, 2009. Further, Cabinet Committee on Security has in principle approved the DetailedProject Report of NATGRID on June 6, 2011. Ministry of Home Affairs, Nov. 27, 2012, Press Information Bureau, Government of India, *available at* : http://pib.nic.in/newsite/mbErel.aspx?relid=89574 (last visited on Nov. 15, 2016).

62 "Let me assure the house that Aadhaar's linking with NATGRID is not there, said Ravi Shankar Prasad, adding that the government even refused to handover the biometric details even when it was approached by the CBI". *DNA*, Apr. 11, 2017, *available at*: http://www.dnaindia.com/india/report-aadhaar-not-to-be-linked-with-national-intelligence-grid-ravi-shankar-prasad-2394742 (last visited on Apr. 12, 2017).

a holder in relation to his biometric information or demographic information, on being submitted by any 'requesting entity'. A 'requesting entity' has been defined under section 2(u) to mean an agency or person that submits the Aadhaar number, and demographic information or biometric information, of an individual for authentication. Section 8(4) further provides that the authority shall respond to an authentication query with a "positive, negative or any other appropriate response sharing such identity information excluding any core biometric information". While a response in the affirmative or negative may suffice for authentication of information, it defies imagination as to why the authority would consider sharing any identity information with any requesting entity, which entity is in any event vaguely defined under the Act. Such usage has to be viewed in the light of section 57 of the Act which enables use of Aadhaar number for establishing the identity of an individual for any purpose, whether by the state or a body corporate or person. Such concerns about use of personal information by private entities for uses not related to state subsidies are not notional either. Swabhimaan Distribution Services Pvt. Ltd., a company incorporated in 2011, is offering services[63] such as authentication of identity, scanning of court records, profiling social media, employment background check to name a few,[64] using Aadhaar number, permanent account number and biometrics. The services offered by this organization are disconcerting as it invites anybody not only to verify a data subject's Aadhaar identification but also to share the details of such verified data subject through text messages and common messaging platforms like WhatsApp.[65] Swabhimaan Distribution Services Pvt. Ltd. proudly claims to be doing this with the benevolence of the authority.[66] Indeed the authority seems to be quite enthusiastic about utilization of Aadhaar number for authentication beyond public subsidies. A convenient handbook[67] published by the authority narrates the details pertaining to

---

63 *Available at*: https://www.trustid.in (last visited on Apr. 17, 2017).

64 *Id.*, "Trust ID offers instant Aadhaar ID authentication or Aadhaar ID background check for any contact. TrustID can be used to check anyone's Aadhaar ID in various situations ranging from hiring a domestic help like maid, cook, driver, *etc.* to giving out property on rent or recruiting an employee … verify anyone using their Aadhaar ID in less than 1 minute."

65 *Id.*, "(E)nd user can also share details of the verified contacts through WhatsApp / SMS etc. Specific service experiences can be rated and reviewed by the end user too."

66 *Id.*, "…Swabhimaan Distribution Services Pvt. Ltd. (www.swabhimaan.com), which is a registered Authentication User Agency (AUA) with UIDAI."

67 Aadhaar Authentication User Agency (AUA) Handbook - Version 1.0, Jan. 2014, *available at*: https://www.uidai.gov.in/images/aua_handbook_v1.0_final_30012014. pdf (last visited on Nov. 15, 2016).

accreditation as an 'Authentication User Agency', a term conspicuous by its absence in the Aadhaar Act. The authority seems to distance itself from being merely a vehicle for delivery of subsidies, benefits and services borne off the consolidated fund of India and an authentication user agency is invited to "consume or offer authentication services for resident service delivery".[68] This handbook claims that the "Aadhaar authentication service responds only with a yes/no and no Personal Identity Information is returned as part of the response"[69] which, on the face of it, is contrary to what is set out under section 8(4) of the Act. The publicised authentication service offered by the authority may be depicted[70] as follows:

Personal Data	***Authentication Result***	
Aadhaar Number	+ Biometric Information	YES or NO
	+ Demographic Information	
	+ PIN/One-Time Password (any or all of the above)	

The Aadhaar Act may not permit the authority to share biometric data collected under the Act. But that does not preclude any private third-party from demanding biometric data from a person as a condition for any goods, service or even employment. The third-party may, through an authentication user agency, seek verification/authentication as above. Consequently, even if the authority responds only with an affirmative or a negative response, the authentication user agency will ultimately have an officially verified record of Aadhaar number and the correct biometric and demographic information linked with that Aadhaar number.[71] The Act does not impose any obligation on subsequent

---

68 *Id.* at 4.

69 *Ibid.*

70 *Id.* at 5.

71 "Demographic authentication wherein the Aadhaar number and demographic data of the Aadhaar number holder in the database of the requesting entity or as obtained at the point of authentication is matched with the demographic attributes (name, address, date of birth, gender, etc) of the Aadhaar number holder in the CIDR and response returned as a "Yes" or "No" along with other information related to the authentication transaction. Biometric authentication wherein the biometric data along with the Aadhaar number submitted by an Aadhaar number holder are matched with the biometric attributes of the said Aadhaar number holder stored in the CIDR and return a response in either a "Yes" or "No" along with any other information related to the authentication transaction." Authentication Overview, Unique Identification Authority of India, *available at* : https://uidai.gov.in/authentication/authentication.html (last visited on Apr. 17, 2017).

retention or usage of this verified data by such third-party/agency. Nor does the Act prevent sharing of data so collected by the third-party subsequent to its verification by the authority. A practical manipulation of this is evident from the services offered by the Swabhimaan Distribution Services Pvt. Ltd. which advertises the ability of its users to share verified data.[72]

So far as the assertion of a mere yes/no response is concerned, this author accessed the official website of the authority which provides free of any charge public services pertaining to Aadhaar data verification;[73] upon input of just his Aadhaar number, the result was not merely a yes/no response but his gender, a ten-year age bracket that he fell in, his state and the last three digits of his mobile phone number. It may also be pointed out that these public services do not set down any prior conditions whatsoever for their use; all that was required was merely an Aadhaar number, which does not speak very highly about data protection mechanism put in place by the authority.

In 2016, the High Court of Delhi was considering the privacy of data relating to users of mobile messaging application, WhatsApp in the background of acquisition of WhatsApp Inc. by Facebook Inc.[74] The issue related to personal data which had been collected and stored by WhatsApp, to be transferred to its new parent entity, Facebook. While declining to entertain the larger question of right to privacy, the court directed WhatsApp not to share existing information/data/details of users up to Sep. 25, 2016 (the date on which WhatsApp effectively modified its privacy policy) while at the same time, shifted the onus on WhatsApp users to delete their data subsequent to Sep. 25, 2016. The events demonstrate the opposition towards data protection in India as apparent from news reports suggesting that that this widely used messaging service, WhatsApp, is prepared to share data with its parent Company, Facebook, judicial directions notwithstanding.[75] This decision of the High Court of Delhi

---

72 *Supra* note 61.

73 *Available at*: https://resident.uidai.gov.in/aadhaarverification (last visited on Apr. 17, 2017).

74 *Karmanya Singh Sareen* v. *Union of India*, 2016 SCC OnLine Del 5334 : MANU/DE/2607/2016.

75 "Defying Delhi high court order, WhatsApp to share data with Facebook" *The Hindustan Times*, Sep. 29, 2016, *available at*: http://www.hindustantimes.com/india-news/defying-delhi-high-court-order-whatsapp-to-share-data-with-facebook/story-M2jdggChtooHduB87cd6hN.html (last visited on Oct.1, 2016).

has been challenged before the Supreme Court of India[76] and pending adjudication as of May, 2017.

It is evident that manipulation of Aadhaar data by private entities ought to be unambiguously and strictly regulated under the Act. While the Act may call upon 'requesting entity' to inform a data subject of alternatives to identity information, in practice, and with unequal bargaining power, the Aadhaar number may well end up becoming another *de facto* identification criteria for purposes never envisaged when the law was enacted. This has to be also considered with the fact that an individual data subject has no mechanism of redressal of grievances under the Act. The scope of data shared and entities with which data may be shared ought to be restricted under the Act itself in conformity with its stated policy and purpose to the extent that it can be gathered from the preamble[77]of the Act. The Aadhaar Act has introduced some of the basic principles of data protection to India and while it has the potential to lead development, or at least an informed debate on data protection laws in India, there is an imminent need to place checks on the use of Aadhaar data by private entities, which, as of now, is bordering on the reckless.

VIII The blueprint of life

Analysis of DNA is reputed as one of the perfect forensic analysis tools to individualize amongst a population, to the extent that DNA profile is considered unique with reasonable scientific certainty.[78] In the year 2012, a non-governmental organization approached the Supreme Court of India in *Lokniti Foundation* v. *Union of India*[79] on the issue of profiling DNA of unidentified human bodies or victims of kidnapping to find possible DNA matches with people who had reported missing persons. In 2014, it was submitted on behalf of the Union of India that the Ministry of Science & Technology, Government

---

76 *Karmanya Singh Sareen* v. *Union of India,* SLP (C) No.804/2017, Supreme Court of India. This matter is pending before the court.

77 "An Act to provide for, as a good governance, efficient, transparent, and targeted delivery of subsidies, benefits and services, the expenditure for which is incurred from the Consolidated Fund of India, to individuals residing in India through assigning of unique identity numbers to such individuals and for matters connected therewith or incidental thereto." The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

78 "Current DNA short tandem repeat (STR) profiling techniques … the MPs [match probability] for individuals unrelated to the defendant are extremely small, often less than one in a billion." Christophe Champod, "Identification and Individualization" in Alan Jamieson, Scott Bader (eds.), *A Guide to Forensic DNA Profiling* 70 (John Wiley & Sons, 2016).

79 W.P. (C) Nos 491/2012.

of India was working on a Human DNA Profiling Bill for establishing a National DNA Data Bank, a DNA Profiling Board for the use of DNA profiles. The bill proposes to maintain confidentiality of such DNA data bank and use it for law enforcement purposes and in judicial proceedings (whether for prosecution or defence). It may also be used for maintenance of population statistics, research and quality control, provided that personally identifiable is not used for such purposes. The bill also proposes use limitation principle insofar as it restricts use of DNA profile only to purposes set out in the bill. Subject to the conditions set out in the bill, even a person convicted of an offence may apply to the court seeking DNA profiling of specific evidence. Unauthorized disclosure or obtaining of DNA data is proposed to be punished with simple imprisonment for not less than one month but up to three years and also fine up to Rs. 1 lakh. Destruction, alteration or contamination of biological evidence is a punishable offence, though, to constitute an offence, it requires knowledge or intention.

IX Conclusion

Considering that data protection is not a completely unexplored phenomena, in the light of the enactments discussed above, it is surprising to find rather rudimentary and uninspired proposals as the Personal Data Protection Bill, 2006,[80] the Right to Privacy Bill, 2010 [81] and the Personal Data Protection Bill, 2014,[82] all introduced as private member's bills. Sectoral legislation in India, such as the Information Technology Act, 2000, the Credit Information Companies (Regulation) Act, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act,

---

80 Bill No. XCI of 2006, as introduced by Vijay Jawaharlal Dardain the Rajya Sabha on Dec. 8, 2006. The bill aims "to provide for protection of personal data and information of an individual collected for a particular purpose by one organization, and to prevent its usage by other organization for commercial or other purposes and entitle the individual to claim compensation or damages due to disclosure of personal data or information of any individual without his consent."

81 Bill No. LX of 2010, as introduced by Rajeev Chandrasekhar in the Rajya Sabha on Feb. 25, 2011 seeks to "provide protection to the privacy of persons including those who are in public life". Though the bill states that its objective is to protect individuals' fundamental right to privacy, the focus of the bill is on the protection against the use of electronic/digital recording devices in public spaces without consent and for the purpose of blackmail or commercial use.

82 Bill No. XXIII of 2014, as introduced by Vijay Jawaharlal Dardain the Rajya Sabha on Nov. 28, 2014 aims "to provide for protection of personal data and information of an individual collected for a particular purpose by one organization, and to prevent its usage by other organization for commercial or other purposes and entitle the individual to claim compensation ordamages due to disclosure of personal data or information of any individual without his consent."

2016, the Right to Information Act, 2005 and the Consumer Protection Act, 1986, broadly recognize the fundamental principles of data protection in collection and use limitation, retention, rectification, subject access, security and remedies. It may not be far-fetched to say that these legislations can lay down the building blocks of a comprehensive data privacy law for India. The Information Technology Act and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 play a vital role in data protection by securing electronic data and the Credit Information Companies (Regulation) Act aims at achieving data accuracy and privacy. The grievance redressal models from Consumer Protection Act and the Right to Information Act can supply the most essential aspect of data protection by providing speedy, easily accessible and effective remedy to a data subject.

While the Aadhaar Act does provide for data protection measures, a debate appears to be directed at perceived intrusion in privacy of personal affairs by the state. Considering the restrictions placed on the state under the Act and that the constitutional courts of the land remain the guardians of personal liberties against state intrusion, it is the practically unregulated use of personal data by private entities which is a bigger cause for concern. Data protection fundamentals applicable to the state ought to be applied unambiguously in equal force to such private bodies. The Aadhaar Act has shaped into a contentious debate as well as a strong reminder for data protection law in India and may well turn out to be the watershed in the course of privacy laws in India.

*Atul Singh**

---

* Ph.D. Scholar, Faculty of Law, University of Delhi.