pISSN: 2454-7107, eISSN: 2455-4189

Indian Journal of Law and Human Behavior
Volume 4 Number 1, January - June 2018
DOI: http://dx.doi.org/10.21088/ijlhb.2454.7107.4118.13

Review Article

Privacy, Human Behaviour and Fundamental Rights in India: Some Recent Developments and Analysis

Sheshadri Chatterjee

Author Affiliation
Research Scholar and LLM Professional, National Law University Delhi, New Delhi, Delhi 110078, India.

Reprint Request
Sheshadri Chatterjee
Research Scholar and LLM Professional, National Law University Delhi, New Delhi, Delhi 110078, India.
E-mail:
sheshadri.academic@gmail.com

Received on 23.02.2018
Accepted on 09.03.2018

Abstract

In this era of digitalization as well as Information and Communication Technology (ICT) where there exists innumerable flow of data, the part played by issues connected with data privacy plays a crucial role. The very question relating to the conception of privacy in Indian context is not clear, nor there is any clear definition of 'personal data' anywhere in the jurisprudence. The conception also could not be made clear even by studies of the Constitution of India since in so many words it has yet not dealt with "right to privacy". However, different cases in Supreme Court and High Courts of the States always observed that "right to privacy" should get place in a univocal form in the Constitution of India. This study has taken a holistic attempt to elucidate the meaning of privacy through different angles and perspective and discussed how the authority has gained competence to enact laws relating to data privacy like IT Act 2000 and gave a detail insight mentioning judicial references as to how privacy has become close to not only sense of Article 21 of the Constitution of India but also throughout the entire Part III of the Constitution of India. This study also discussed IT Act, 2000 with its amendment relating to privacy issues including discussion of latest full bench judgement regarding right to privacy followed by providing a recommendation to be followed for ensuring privacy protection. The study is ended with a meaningful concluding remark.

Keywords: Data Protection; Fundamental Rights; Human Behavior; Personal Data; Privacy.

Introduction

In this online environment when all transactions including commercial and otherwise are taking place in cyber space, it is evident that there will be influx flow of data. During such ceaseless flow of data, the probability of data theft engineered by some unscrupulous persons cannot be set at naught. To keep this menace in check or even for its total annihilation, authority is to be honest in framing appropriate policy and regulations in an unambiguous ramification. This burning issue of data theft endangering breach of privacy is in existence globally [1]. If we take the trouble to hazard our curiosity in this area, we will find that initially this issue of protection of privacy concerning to data arose in Northern European countries [2] and in degrees, the idea spread over other areas even across the border right from early 1990s [3] though at the initial stage all the data protecting authorities started

dealing with those data which are non-sensitive in nature [4]. In India, the necessity of data protection privacy policy grew owing to keep the menace of data infringement in check especially in cases of protection of those data which are exported by the foreign organizations to India to their Indian counterparts to whom the foreign organizations outsourced those data in the present outsourcing environment paradigm. It is pertinent to mention here that more data would cross the border, greater would be the chance of occurrence of data theft culminating infringement of data privacy [5,6]. Thus, to combat data theft causing privacy infringement, India is needed to provide robust policy and to take attempt to frame simple enactments. Enactments are framed usually having sanction and empowerment endowed from the recital of the Constitution of India which is construed to be parent body for providing idea and power to the appropriate authorities for framing policy and for framing congenial regulations.

Ironically, in the Part III of the Constitution of India where there exist some fundamental rights, it appears that mentioning of right to privacy explicitly is absent. In absence of such, relating to right to privacy, many litigations cropped up and those were settled through judicial interferences. We will mention those in brief in subsequent stages. However, in the month of August 2017, the full bench of the Supreme Court of India delivered a revolutionary judgement, K.S. Puttaswamy and others v Union of India[7]and others, wherein it was held that right to privacy is a fundamental right though this right was not declared absolute right.We will discuss it later in detail. The objective of this article is to provide an insight as to how different enactments, judicial precedence and Constitution of India provided safeguards to protect privacy in the ceaseless data flow system in this digitalized society where use of new technologies like Internet of Things as well as Artificial Intelligence (AI) involving exchange of Big Data have enhanced the necessity of data protection.

Meaning of Privacy and Its Conception

The definition of privacy can be conceptualized through the sense in which one is wanting to interpret it. Context is important. Many definitions of privacy are there provided by the scholars. There are three approaches in defining privacy which are Structuralist Approach, Individualistic Approach and Integrative Approach. So far as Structuralist Approach is concerned, privacy has been defined as "Privacy denotes a degree of inaccessibility of persons, their mental status, and information about them to the senses and surveillance devices of others" [8]. Also, privacy has been defined as, "privacy is a condition of being protected from unwanted access by others" [9]. So far as Individualistic Approach is concerned, privacy has been defined as, "claim of individuals, groups or institutions about them is communicated to others" [10]. Privacy has also been defined as, "information control and control over decision-making [11]". So far as Integrative Approach is concerned, privacy has been defined as, "an important interest in simply being able to restrict information about, and observation of myself regardless of what may be done with that information or the result of that observations [12]".

This definition helps us to understand that Integrative Approach is a combination of Structuralist Approach and Individualistic Approach. Interestingly, the very nomenclature 'Integrative' signifies the sense of this combination. Whatever approach is considered in defining privacy, conception of privacy contributes some essential values to the society [13].

However, regardless of the wordings of definition of privacy, it is a fact as to how one is conceptualizing relating to infringement of privacy is an important consideration. It varies from individual to individual, it differs from place to place depending on the societal system and diversified culture [14] where one lives in so far as Indians are concerned. Besides, it is experienced that Indians are more concerned with privacy which covers privacy of physical space, privacy of living space whereas people of western countries are sensitive in privacy issues relating to security and privacy of data as well as of Information [15,16,17]. Thus, it is clear even in India specific thinking is important - what is considered for me infringement of privacy, it may not be considered so by you. Again, in India, conception of privacy also depends on gender division. I am not going to elongate my discussions in this regard more. However, it can safely be inferred that right and sense of privacy can hardly be weighed, calibrated and standardized since it depends on the conception and interpreting capability of an individual, since these as intangible issues.

Data Privacy and Its Need in India

Data privacy issue in India is a new concept. This need of data privacy in India has been evolved for different necessities. The online activities in India are growing rapidly. People have become savvy to use cloud platform for instant purchase of items. The online players are also releasing different concessions to the prospective consumers to make the online

activities more lucrative. Online activities are associated with exchange of personal information as well as of financial information of the consumers.

Exchange of data is taking place in such e-commerce activities. Consumers are found hesitant to be involved in such activities without being sure that their data would not be misused nor would be infringed by unscrupulous persons. Unless that much of trust is grown among the minds of the consumers, enhancement of e-commerce activities in India cannot be achieved [18]. The e-commerce players felt it and are trying to plug-up any possible pilferage for protecting data. When the consumers express implicitly or explicitly any doubt regarding their data safeguard, they become hesitant in using online platform and start sincerely regulating them to protect their data and this would reduce the online activities of the consumers [19,20]. They would, in such case, exhibit negative behavior towards sharing of their personal data in the virtualplatform [21,22,23]. The awe of online consumers has become instrumental in emphasizing the need of data privacy. There is another bigger front which demands the need of ensuring data privacy. This is emanating from the ever-expanding offshore business paradigm conducted in India by the foreign organizations. In this scenario, important data of foreign organizations are outsourced to the Indian organizations [24]. This outsourcing business has covered a lucrative market in India and this has given rise to many job opportunities. Now if the offshore organizations exporting data to their counterparts in India do not feel confident that their exported data would be properly protected, they would exhibit negative gesture towards such outsourcing issues. This will highly inhibit this business market in India.

This issue has provoked the Indian authorities to feel the need of ensuring data privacy and as such, they are relentlessly trying to arrange to devise tools and laws of data protection in India. Another important aspect deserves mentioning here which also motivated the feelings of the authorities of India for being sincere for safeguard of data. The new technologies known as Internet of Things (IoT) and Artificial Intelligence (AI) are gradually grabbing the IT markets in India [25]. Here, through execution of IoT activities, influx of data will be exchanged, and such exchange of innumerable data called Big Data should be properly managed to protect against data breaches.

Again, the AI technology is important in the light of data protection activities since the AI technology is associated with decision making. If exchange of Big Data through AI is not properly protected, the corresponding decisions which would be adopted by AI technology will be highly prejudicial and will be inimical for the society. Thus, it can be said that for different reasons as discussed above, Indian authorities are interested in ensuring to establish appropriate data privacy mechanisms. Be it mentioned here that for protection of data, different enactments have been framed. The Information Technology Act, 2000 has been duly amended to address the situation which is believed to have been able to some how manage the situation though meaning of "personal data" has not been exclusively elucidated in that act. Moreover, Credit Information Companies (Regulation) Act, 2005 has been framed to protect data to some extent as its provisions appear to not have explicitly dealt with privacy protection of information. However, a general Data Protection Act is to be framed to cover all possible points for ensuring full-proof data privacy.

Constitutional Scenario Regarding Privacy

The constitution of India came into force in the year 1950. Before that, in India, during independence period, the issues covering infringement of privacy were dealt with the help of existing criminal laws, especially covering unchastity actions to women, relating to affairs of properties. These were construed to be offences punishable in laws. At that period, law of torts also played vital role and acted as a substantial weapon to address infringement of privacy. However, privacy hampering one's name and fame was not protected legally [26].

Ironically, even after enforcement of Constitution of India in 1950, right to privacy was not guaranteed as fundamental right. Different judicial decisions became instrumental in interpreting the constitution of India covering Part III (Articles 14 to 30) in terms of establishing privacy right though in some specific contexts like unauthorized telephone tapping, People's Union for Civil Liberties (PUCL) v. Union of India [27]; like, collection of evidence through illegal search was not construed as infringement of privacy as it did not infringe any fundamental right to privacy, Puranmal v Director of Inspection (Investigation) of Income Tax [28], New Delhi. Several other judicial decisions interpreted different Articles under Part III of the Constitution of India to cover right to privacy. It is seen that Article 21 of the Constitution of India has been interpreted in the judicial decision of Supreme Court of India, M.P. Sharma v Satish Chandra [29] wherein right to life and liberty as enshrined in Article 21 can be protected if any action is taken without taking appropriate procedures established by law since the recital of

Article 21 envisages as, "No person shall be deprived of his life or personal liberty except according to the procedure established by law". This Article 21 encompasses negative injunction relating to positive mandate. It has allowed to perform all things which would associate to lead a life with dignity as cited in Maneka Gandhi v Union of India [30]. In this way, the judicial decisions covered right to privacy though explicitly this right was not depicted in the literature of Constitution of India. To cover protection to right to privacy in the affairs of data theft, Information Technology Act, 2000 has been framed and subsequently amended in 2008 for providing penal provisions to implicate delinquents who are involved in commission of data theft. Question arose if the Constitution of India gave power to the law-making authority to legislate this type of Act like I.T. Act, 2000 since in the Constitution of India under Article 246 there exists List I, List II and List III which do not empower the Parliament or State Legislative Assembly to frame laws concerning to data privacy and data protection. However, the entries in these Lists can be amended through rigorous procedure laid down in Article 368 of the Constitution of India, but without taking recourse to that, how the Parliament of India enacted I.T. Act, 2000 was a question.

Even if we focus attention to the entry no. 97 of List I which is said to be Union List, it appears that in entry 97 it is depicted, "Any other matter not enumerated in List II or in List III including any tax not mentioned in either of these Lists". Then how the authority could frame I.T. Act, 2000 which covers data protection? However, the decision of the Supreme Court in Union of India v H.S. Dhillan [31] paved the way because it was held there that the parliament can enact in terms of residuary power laid down in article 248 of the Constitution of India if the legislation does not come under List II or in List III.This has also been confirmed in another judicial decision, Attorney General of India v Amratlal Prajivandas [32]. Thus, there appears to be no impediment legally in framing I.T. Act, 2000 which ensures privacy protection of data in this modern society where there exists flow of innumerable data of multipurpose nature in online environment. However, here no further discussions are taken regarding pros and cornsof I.T. Act, 2000, but discussions are confined regarding constitutionality of the right to privacy.

The Full Bench Judgement and Analysis

On 24 August 2017, the full bench of the Supreme Court of India issued judgement conferring right to privacy as fundamental right. The judgement appears to be a very important judgement, K.S. Puttaswamy and others v Union of India [33] andothers wherein the full bench through observations spreading over 547 pages discussed in broad spectrum covering the values of dignity and liberty in dealing with constitutionality regarding right to privacy. The full bench pulled the system of maintenance of right to privacy in different western countries like US, UK and so on and synthesized how the right to privacy is carefully preserved in those respective legal systems. The full bench sincerely emphasized the need of importing the right to privacy in the constitution for protection of privacy in the firmament of Indian jurisprudence. The said valued judgement took help of the preamble of Constitution of India which was eventually declared part of the Constitution in terms of decision in Kesavananda Bharati v union of India [34]. The full bench took the term "Dignity" as depicted in the preamble of the Constitution.

The judgement cited the decision of US court where it was observed that life is required to be construed as, "more than mere animal existence", as cited in the case of Munn v. Illionoss [35]. The full bench also cited another decision of the Supreme Court, cited in A.D.M. Jabalpur v. Shiv Kanta Sukla [36] where it was observed *interalia* that "privacy is a natural right". The full bench rigidly and rightly discarded the smaller bench decisions cited by the ld. Attorney General of India defending the interest of the Union of India where privacy was not given fundamental right, as cited in M.P. Sharma v Satish Chandra [37] and in Kharak Singh v. State of UP [38] since the decisions came out not from the full bench but from smaller benches of the Supreme Court of India comprising of eight and six judges respectively. The full bench observed *inter alia*, "…Liberty has a broader meaning of which privacy is a sub set…".

Eventually, after a long discussion citing many instances and multipurpose references, the full referral bench of the Supreme Court of India on 24 August 2017 delivered this valued judgement holding that privacy is construed to be a fundamental right in terms of Article 21 of the Constitution of India and unanimously opined that this right to privacy being fundamental in nature is instrumental to be applied in the sense of all the Articles covered under Part III of the Constitution of India. This branded and valued judgement is considered by the judicial elites to be a remarkable document dazzling in the azure of Indian jurisprudence. Ironically, the court did not confer this right to privacy as an absolute fundamental right but declared it as fundamental right on the

contrary. It would have been, it is humbly submitted, better had the Supreme Court of India would have been pleased to issue the order making this right as 'absolute' right. The salient points of this important judgement are briefed below.

a. Life and personal liberty cannot be separated. There are inalienable rights. These rights are essential for human existence with dignity. Dignity, equality and liberty are the three principal plinths of the Constitution of India.

b. Sense of personal liberty and life has not been created by the Constitution of India, but these have been implicitly recognized by the Constitution of India since these are construed to be intrinsic and inseparable parts of human life.

c. Essence of guarantee of life and personal liberty is envisaged in Article 21 of the Constitution of India and the sense of privacy is consequential outcome of guarantee of life and personal liberty. Slightest culture of other rights enshrined in Part III of the Constitution of India helps to construe that those rights are eventually converging to focus on the elements of privacy.

d. Privacy is recognized judiciously, and it should not be meant that the apex court is amending the Constitution of India illegally encroaching the inherent jurisdiction of the Parliament of India, but the sense of fragrance of privacy is spread in every line of the Part III of the Constitution of India.

e. Privacy is instrumental on those precious values shouldering which other freedoms enjoined in Part III of the Constitution of India are founded. Privacy gives some entitlements ascribed through the inner sense of liberty.

f. Privacy emphasizes the right to be left alone. All the personal intimacies of family life are associated with the sense of privacy. Essential aspects of human lives are controlled by this ingredient. Privacy acts as a vital protector of heterogeneity of human culture. Privacy comes out from the sense of dignity. Privacy is spread everywhere in human life–from intimate to private, from private to public areas.

g. The interpretation of the Constitution of India should be befitting with time. The idea of inner meaning of the Constitution of India has been changed with enormous technological progress to fit with the present situations and right to privacy is required to be interpreted through the Constitution of India accordingly. Interpretation of the Constitution of India must be, as such, flexible. In future, the interpretation would be or may be otherwise befitting with the situation and as such, its amplitude of interpretation should be construed to be infinite.

h. Privacy is a fundamental right but not absolute right. Can be infringed if actions taken legally if actions taken according to need in terms of and in consequence with state aim and if actions taken in terms of proportionality ensuring appropriate and rational nexus concerning to objects and means required to ensure as well as to achieve the objects.

i. Privacy may be construed to function in positive as well as in negative way. To protect the privacy of individuals by the state is positive function whereas intrusion upon the life and personal liberty of individuals is to be restrained by the state which is construed to be negative function.

j. Information privacy is also included in the right to privacy under the changed modern technological ambiance. Data protection is required to be ensured by the Union Government. A well-defined balance is to be ensured between interest of the individual for privacy protection and legitimate concerns of the state.

Different Scenarios Involving Privacy Issues and Constitution of India

The Supreme Court of India, in many cases, has elucidated the inner meaning of the recital of Article 21 of the Constitution of India. In course of different judicial decisions in different contexts dealing with application of Article 21 of the Constitution of India, the supreme Court of India widened the amplitude of applicability of this Article and provided a calibrated and meaningful guideline for dealing with right to privacy in different litigations under different varied contexts. These are as follows.

a. Telephone tapping being construed as invasion of one's right including its requirement as public safety and that is to be covered with procedural safeguards.

b. It is an obligation of private medical establishment or Government hospital to provide medical protection or to help medically to an injured person.

c. Denial of medical help from the end of government hospital to an injured person amounts to violation of Article 21.

d. It is the duty of the public and private industries to arrange to improve health of their employees and for this regular medical check-up is to be provided to them.

e. If an individual is honestly incapable to pay any

debt, he cannot be imprisoned.

f. It may be argued that "right to die" or "right to commit suicide" though not included in Article 21 but Section 309 of Indian Penal Code covers it which is also not violative of Article 21 of the Constitution of India.

g. State has the obligation to issue permission for opening of Law College (Private) and to arrange to give them grant-vs-aid.

h. An individual should be only handcuffed when there is chance of his escape.

i. If there is long delay (to be decided by Court) in executing death sentence, it would pull protection attributed under Article 21 of the Constitution of India and that death sentence to be converted to life imprisonments.

j. Protections of life and protection of liberty as envisaged under Article 21 of the Constitution to be applied to persons who are not citizens of India.

k. It has been also held that capital punishment does not violate provisions of Articles 14, 19 and 21 of the Constitution of India.

l. Hanging should be construed to be fair and not violative of Article 21.

m. It tantamount to denial of Article 21 of the Constitution of India when a working woman is harassed sexually in her workplace.

Recommendations on Issues Concerning Privacy to Different Authorities

To achieve success in data privacy in cyberspace, the relevant players in the cyberspace are required to work with close liaison lest there may not occur any dislocation. The relevant players in the cyberspace relating to enforcement of data privacy include public and private sectors who are scheduled to work in tandem to establish congenial culture for maintenance of full-proof data privacy in cyberspace. For this, both public and private sectors are to be sincere and meticulous to adhere to some salient issues which will be described here in brief. By public and private sectors it is meant Government of India who are responsible to maintain and mechanize data privacy management in an effective and calibrated way; law Enforcement Bodies who are responsible to keep them updated for amendments of existing laws concerning to data privacy to aptly combat the needs of the society keeping pace with rapid advancement of technology, Industries who should ensure development of culture among their employees for ensuring data privacy and also to ensure congenial practices among the employees for taking appropriate steps for protection of data; Organizations dealing with data exported by overseas organizations in the form of outsourcing where the organizations are required to be sincere and serious in dealing with those data so that the foreign concerned organizations feel safe in the protection of privacy of their data so outsourced. However, the entire mechanisms are depicted below serially.

Government Authorities

The authorities should be vigilant in aptly amending Information Technology Act, 2000 which is instrumental for regulating data privacy management. The activities must be liberal in incentivizing research works for prescribing updated practices which might ensure appropriate data privacy management. They should formulate effective, simple, implementable guidelines for protecting data and they should keep them refreshed and updated regarding ever-changing global legal systems for appropriately mitigating occurrence of privacy infringements by the unscrupulous persons. The responsibilities of Government Authorities in this context are stated below in seriatim.

a. More effective and robust amendment needed in I.T. Act for data privacy withclear and pragmatic penal provision including personal data privacy.

b. To ensure transparency in privacy protection, all government agencies need to be included in defining 'Body Corporate' as enjoined in I.T. (Amendment) Act, 2008 (Sec.43(A)).

c. To establish a national ecosystem for non-stop engagement for the cause of data protection [39].

d. More investment to be made in research works covering issues of data management and privacy [40] so that all the stakeholders possess updated information.

e. End users to be made more aware for which proper training is needed.

Law Enforcement Authorities

Law enforcement authorities are to be sincere to keep them updated and aware relating to progress of modern technologies to enhance their self-regulating capabilities to address privacy infringements of personal data. This is essential to face the delinquents who might adopt modern technologies to infringe personal data. They should be well equipped with

ever-changing global relevant regulations so that they can draft befitting regulation in keeping with such changing global regulation scenario. It will be their responsibilities to keep the potential users aware regarding modern techniques which might be adopted by the infringers so that the potential users can act accordingly and may make them proactive to face any untoward situation whatsoever.

The responsibilities of the Law Enforcement Authorities are depicted below in seriatim.

a. Implementation of projects to be done following strictly privacy policy.
b. In the process of data collection, use, processing and storing, privacy to be ensured.
c. Development of proper culture for maintenance of privacy.
d. Law enforcement authorities are to upgrade them relating to updated techniques of data flow mechanism so that they do not face any impediment to enforce laws.
e. End users to be kept aware regarding menace of cybercrimes.
f. Amend laws appropriately with cultural and other changes of the society relating to the data protection issues.

Industry and Regulatory Authorities

Industries must ensure appropriate practices and processes for data privacy mechanisms and should train their employees accordingly so that they can feel the privacy needs of the industries and can act in appropriate manner to plug-up any chance of occurrence of privacy infringement. The industrial authorities are required to keep close contact with the Government authorities to make them appropriately updated with latest privacy policy of the Government so that there might not be any unwanted gap in the close relation. The responsibilities of Industries and Regulatory Authorities are depicted below in seriatim.

a. Industry practices to be effectively controlled regarding implementation of standardized process of privacy protection mechanism.
b. Effective mechanisms to be catered for remedies of problems of end users regarding privacy issues in a smooth way.
c. To realize privacy needs for industry and to proceed accordingly.
d. To lobby with the government authority for privacy-policy response.
e. To monitor govt privacy policy for fetching good result.

Outsourcing Organizations

Since the Indian organizations working in IT sectors especially deal with data outsourced by overseas organizations, the concerned authorities are to be sincere in updating their employees in matters relating with privacy policies which are globally acceptable. The employees are to be regularly brushed-up with privacy protection culture so that the employees can sharply respond to any complaint by the overseas organizations concerned alleging occurrence of their data breaches. The Indian organizations should adopt practices for data protection which are internationally accepted because this would help create confidence among the overseas players who are exporting their data. The authorities of Indian industries dealing with data outsourced are to keep all stakeholders aware regarding the fact that Indian constitution has already declared privacy as a fundamental right in terms of Article 21 and Part III of the Constitution of India. The responsibilities of the concerned organizations are depicted below in seriatim.

a. Robust and transparent organization practices to be established depending on globally acceptable privacy policies.
b. To develop a meaningful privacy culture in the organization so that quick response may be achieved in case of data breaches.
c. Arrange to develop a congenial mechanism to protect automatically the data outsourced to Indian organizations by foreign countries.
d. The organizations dealing with data outsourced from other countries should develop a mechanism in consonance with global data protection practices.
e. All the stakeholders to be made aware regarding constitutional safeguards of privacy as enshrined in Article 21 of the Constitution in terms of latest apex court's judgement from referral full bench verdict.

Concluding Remark

The Supreme Court of India through its full bench judgement has conferred right to privacy by logical extraction from the recital of Article 21 of the

Constitution of India. However, it also appears that this right has not acquired absolute right because provision is there for being it curtailed in terms of procedure established by law. Again, this right to privacy would not act in case where exists superior countervailing interest. This right, as such, cannot be construed to be a general and absolute right. Many works have been done. Many cases are there. Many of the cases issued opinion in favor of right to privacy including protection of data but, in India personal data protection policy has yet not been developed. Conception of privacy is found different in India compared to that exists in Western countries. It is a fact that I.T. Act 2000 is based in terms of resolution A/RES/51/162 taken by the General Assembly of UNO on 30.01.1997 in consonance with Model Law on e-commerce adopted by UNCITRAL but it does not provide absolute protection of privacy.

The concept "personal data" has not been made clear elsewhere. Even the amendment of I.T. Act would not provide absolute protection to privacy, it is apprehended. Slight study of I.T. Act will reveal that it is more aligned to e-commerce activities as well as cybercrime issues but less aligned with protection of data. Even the Credit Information Companies (Regulation) Act, 2005 contains provision ensuring protection of data but that is also to some limited extent. This Act does not confer right to protection of information.

In India, there does not exist a general Data Protection Act. Data Protection Authority has been established in India. However, it is fortunate that government of India is contemplating to empower Reserve Bank of India (RBI) for imposition of penalty on any credit information enterprise who would act to infringe privacy. Naturally, in that case, the RBI would be construed to act as Data Protection Authority so far as credit information is concerned. However, this is a superficial attempt to safeguard privacy of data, but more detail studies are required to extend full proof protection against infringement of data for protection of privacy and the Constitution is required to be made more explicit in this context.

References

1. Casaló, L.V., Flavián, C. and Guinaliíu, M. "The role of security, privacy, usability and reputation in the development of online banking," Online Information Review 2007;31(5):583-603.
2. It is based on: Bart van der Sloot, do data protection rules protect the individual, and should they? An assessment of the proposed General Data Protection Regulation, International Data Privacy Law, 4 (2014).
3. Frits W. Hondius, Emerging Data Protection in Europe (Amsterdam: North-Holland, 1975) and Herbert Burkert, Freedom of Information and Data Protection (Bonn: Gesellschaft fürMathematik und Datenverarbeitung, 1983).
4. Advisory Committee of Secretary on Automated Personal Data Systems, Records, Computers and the Rights of Citizens (1973).
5. Cranor, Lorrie Faith and Paul Resnick. "Protocol for automated negotiations with buyer anonymity and seller reputation," Netnomics 2000;2(1):1-23.
6. Chang, E.C., and Ho, C.B. "Organizational factors to the effectiveness of implementing information security management," Industrial Management and Data Systems 2006;106(3):345-361.
7. K.S. Puttaswamy and others v Union of India and others [2012] SC WP (Civil) No.494.
8. Allen, A. "Uneasy Access: Privacy for women in a Free Society," Rowman & Littlefield Totowa, 1988;30:226.
9. Bok, S. Secrets: On the ethics of Concealment and Revilation.Panthcon Books, New York, NJ. 1983.
10. Westin, A. "Social and Political dimension of privacy," Journal of Social Issues 2003;59(2):431-53.
11. Decrew, J. "The Scope of Privacy in Law and Ethics,"Law and Philosophy 1989;5(2):145-173.
12. Reiman, J. "Privacy, intimacy and personhood," Philosophy and Public Affairs 1976;6(1):26-44.
13. Eloff, M.M. and Von Solms, S.H. "Information security management: an approach to combine process certification and product evaluation," Computers & Security 2000;19(8):698–709.
14. Hofsted, G. Culture and Organizations: Software of the mind. USA: McGraw-Hill Education, 3rdedn. 1997.
15. Peltier, T. "How to build a comprehensive security awareness program," Computer Security Journal 2002;16(2):23-32.
16. Kruger, H.A. and Kearney, W.D. "A prototype for assessing information security awareness," Computers and Security 2006;25(4):289-96.
17. Kolb, N. and Abdullah, F. "Developing an information security awareness program for a non-profit organization," International Management Review 2009;5(2):103-107.
18. Pennington, R., Wilcox, H.D., and Grover, V. "The role of system trust business-to-consumer transactions," Journal of Management Information Systems, 2003;20(3):197-226.
19. Larose, R., and Rifon, N.J. 'Promoting i-safety: effects of privacy warnings and privacy seals on risk assessment and online privacy behavior' Journal of Consumer Affairs, 2007;41(1):127-49.

20. Rifon, N.J., LaRose, R., and Choi, S.M. 'your privacy is sealed: effects of web privacy scales on trust and personal disclosures' Journal of consumer affairs, 2006;39(2):339-62.

21. Mukherjee, A., and Nath, P. 'Role of electronics trust in online retailing: a reexamination of the commitment-trust theory' European Journal of Marketing, 2007;41(9/10):1173-1202. < http://projeuni.ir/wp-content/uploads/2013/11/c964562sfsf.pdf> accessed on 11 September 2017.

22. Gracff, T.R., and Harmon, S. 'Collecting and using personal data: consumers' awareness and concerns' Journal of Consumer Marketing, 2002;19(4/5):302-18. < http://www.emeraldinsight.com/doi/abs/10.1108/07363760210433627> accessed on 22 August 2017.

23. Hansen, T. 'Consumer adoption of online grocery buying: a discriminant analysis' (2005) International Journal of Retail and Distribution Management, 2005;33(2):101-21.

24. See Jürgen Schaaf and Thomas Meyer, Outsourcing to India: Crouching Tiger Set to Pounce (Deutsche Bank Research), Oct. 25, 2005, available at http://www.dbresearch.com/PROD/DBR_INTERNET_ENPROD/ PROD0000000000192125.pdf (stating that India is the world's most important offshoring location).

25. Rise of the Machines. (2015). The Economist available at http://www.economist.com/news/briefing/21650526-artificial-intelligence-scares-peopleexcessively-so-rise-machines (accessed 29 Nov 2017).

26. Lynskey, Orla. "Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order," International and Comparative Law Quarterly 2014;63(3):569-97.

27. People's Union for Civil Liberties PUCI v Union of India [1997] 1 SCC 301.

28. Puran Mal v Director of Inspector (Investigation) of Income Tax, Delhi [1974] AIR SC 348.

29. M. P. Sharma v Satish Chandra, District Magistrate, Delhi [1954] AIR SC 300.

30. Maneka Gandhi v Union of India [1978] AIR SC 597.

31. The Union of India v H.S. Dhillon [1972] AIR SC 1061.

32. Attorney General (for India) v Amrat Lal Prajivandas [1994] AIR SC 2179.

33. K.S. Puttaswamy and others v Union of India and others [2012] SC WP (Civil) No. 494.

34. Kesavananda Bharati v State of Kerala [1973] AIR SC 1461.

35. Munn v Illinois [1877] 94 US 113.

36. A.D.M, Jabalpur v ShivkantSukla [1976] SCR 172.

37. M. P. Sharma v Satish Chandra, District Magistrate, Delhi [1954] AIR SC 300.

38. Kharak Singh v State of UP [1963] AIR SC 1295.

39. Hone, K. and Eloff, J.H.P. . "Information security policy—What do international security standards say," Computers & Security, 2002;21(5): 402–09.

40. Hu, Q., and Dinev, T. "Is spyware and Internet nuisance or public menace?", Communications of ACM 2005;48(8):61-67.