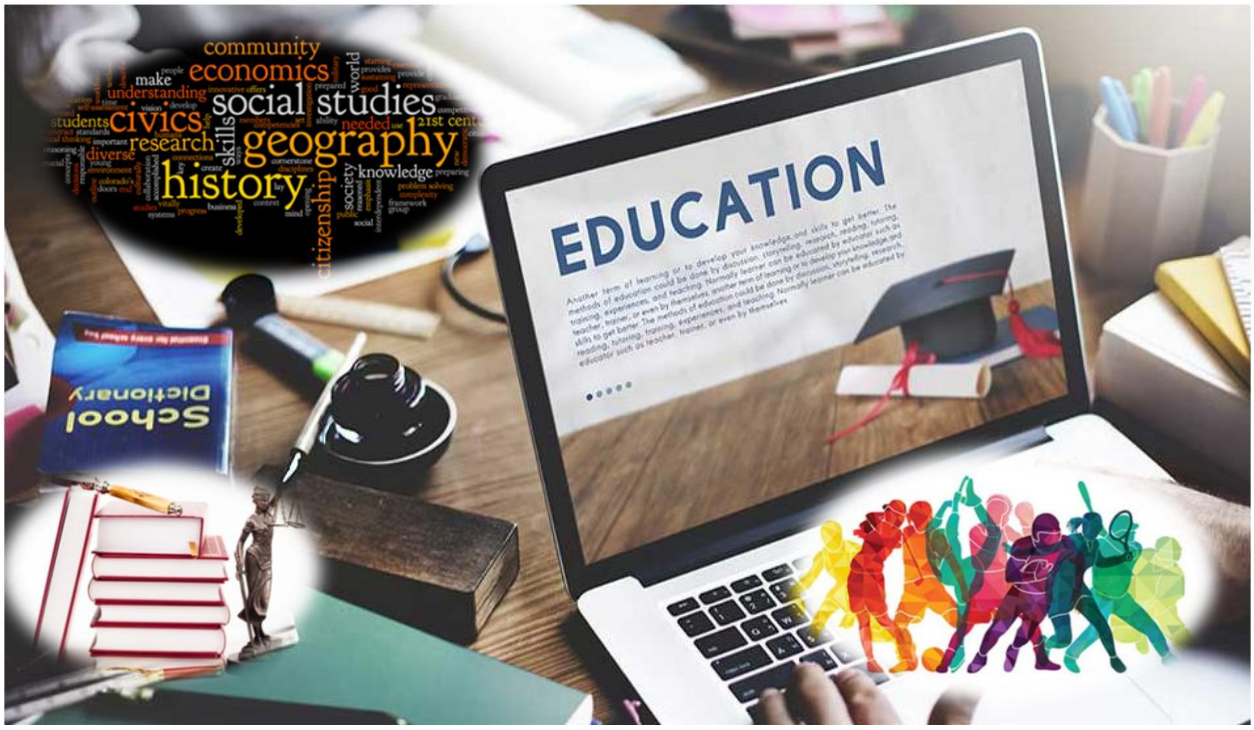


Email:editorijless@gmail.com Volume: 5, Issue3, 2018 (July-Sept)

INTERNATIONAL JOURNAL OF LAW, EDUCATION, SOCIAL AND SPORTS STUDIES (IJLESS)

http://www.ijless.kypublications.com/

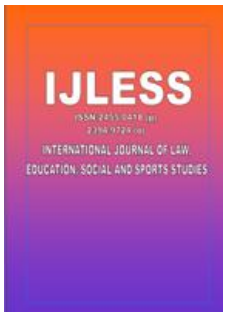
ISSN:2455-0418 (Print), 2394-9724 (online)

www.kypublications.com

International Journal of Law, Education, Social and Sports Studies (IJLESS)
Volume: 5, Issue 3, 2018
ISSN:2455-0418 (Print), 2394-9724 (online)
Research Article

RIGHT TO PRIVACY AND DATA PROTECTION: LAW ALONE IS NOT ENOUGH

RAKESH CHANDRA
Research Scholar, Faculty of Law, Lucknow University



ABSTRACT
The Supreme Court's Judgment of August 2017 is indeed a landmark in the realm of fundamental rights jurisprudence in India. The Court unanimously declared that the right to privacy is a fundamental right and recognised informational privacy as one ofits facets.
The right to informational privacy requires that an individual is able to affirmatively control her life and personality by controlling her personal information. This implies that the law must guarantee an individual the ability to exercise control over the collection, use anddisclosure of her personal information. In the digital age this right assumes enormous significance as the people are sharing huge volumes of personal information to access digitised services.
In the present times, both State and non-State actors alike have access to a citizen's personal data and activities- such as biometric information, internet-use patterns, geometric information, financial information. All this huge data is out there, without a law securing their integrity and protecting the data subject against harm. As the Supreme Court noted, this must be achieved by enacting an effective data protection law for India. Undoubtedly, a comprehensive law on data protection to safeguard an individual's right to privacy is imperative.
On July 31, the central government set-up a five member committee chaired by former Supreme Court Judge, Justice (retd.) B.N. Srikrishna, to draw up a draft Data Protection Bill. One of the primary guiding factors for the committee would be the exhaustive report submitted in October 2012 by a group of experts on privacy led by former Delhi High Court Chief Justice A.P. Shah, which was constituted by the erstwhile Planning Commission. Both the government and the Court have agreed that this would be the "conceptual foundation for protecting privacy" in the form of the new Data Protection Bill.
In the last few months we have read a lot about Aadhar data leak, hacking in Banks and other financial institutions. We are aware also that nearly all the social networking sites have their headquarters in U.S.A. and they are controlling the whole data available on their sites. Further in India also, the maintenance and upkeep of data is in pathetic shape which reminds us of colonial legacy. All these factors poses an important and disturbing question- whether we need a strong Data Protection Law only? Any such Law however strong and comprehensive it might be, cannot account for human element in the upkeep and security aspect of data protection. We badly need a modern and scientific infrastructure for upkeep of data and highly trained staff for the job. We also have to develop appropriate technology for indigenous social networking sites so that our data remains at our hands in our country itself. Lastly, in this age of Artificial Intelligence, we can also think of taking recourse to it in the maintenance and upkeep of the huge data. Only then, the law will prove to be effective in protecting our data and our privacy too.

Keywords: Right to Privacy, Informational Privacy, Committee on Data Protection Bill, Data Protection Law.

Introduction

In a recent judgment a few months ago, the Supreme Court has declared the right to privacy as a fundamental right. This verdict of the nine-judge Constitution Bench of the Supreme Court in Justice K.S. Puttaswami Vs. Union of India[1] has been widely acclaimed as a significant milestone in the jurisprudence on fundamental rights in India.[2]Visualizing the importance of the judgment Prof. Upendra Baxi has rightly stated that "if the 1973 Keshavanand Bharti inaugurated a daringly new constitutionalism for late 20th century India, the R2P affirms, for the 21st century, the vision of a 'constitutional renaissance.[3]"

The Court in its Judgment also recognised informational privacy as one of its facets. The fundamental requirement of the right to informational privacy is that an individual is able to affirmatively control her life and personality by controlling her personal information. This implies that an individual must be guaranteed by law the ability to exercise control over the collection, use and disclosure of her personal information. In this digital age in which huge volumes of personal information is being given up by the people to access digitised services, this right has assumed particular significance. Not only this, state and non- state actors alike have access to a citizen's personal internet-use patterns, geometric information, financial information etc.

In India itself, a number of private enterprises ask employees to mark attendance by putting their thumbs to a fingerprint scanning machine. Phones now unlock themselves reading the user's fingerprints or facial features. When people download and instal apps on their smart phones, they accept all sorts of conditions, including many that invade privacy. Social media open up a great deal of private data. The use of GPS to navigate leaves a trail of one's movements. All this data is out there, without a law securing their integrity and protecting the data subject against harm.[4]

India is one of the key players in the digital and knowledge-based economy, holding more than a 50% share of the world's outsourcing market. Pioneering and technology-inspired programmes such as Aadhaar, MyGov, Government e-market, Digilocker, Bharat Net, Startup India, Skill India and Smart cities are propelling India towards technological competence and transformation. India is already the third largest hub for technology-driven startups in the world and its Information and Communications Technology sector is estimated to reach the 225 billion dollar landmark by 2020.[5]

However, these achievements come with a problem. Innovation in technology, enhanced connectivity, and increasing integration in commerce and governance also make India the fifth most vulnerable country in the world in terms of cyber security breaches according to the Internal Security Threat Report of 2017 by Symantec. Till June 2017, 27, 482 cyber security threat had been reported in the country, according to the Indian computer Emergency Response Team's report. As this is a 23% increase from 2014 figures, it coincides with rapid growth and innovation in the ICT sector.[6] Given the huge number of online users and contained efforts on affordable access, cyber-security needs to be integrated in every aspect of policy and planning.[7]

[1]Justice K.S.Puttaswamy Vs Union of India, 2017 SCC OnLine SC 996, decided on 24.8,2017.

[2] "Saving Privacy for Public Good", by Akriti Gaur & Namrata Mukherjee. Economic Times, dt. 15.09.2017.

[3] Upendra Baxi, 'Opening new doors', The Indian Express, dt.30.8.2017

[4] Economic Times Editorial, 15.9.2017

[5] The Hindu, "For a safe Cyberspace", Subi Chaturvedi, dt. 19.12.2017.

[6]Ibid.

[7] Ibid.

Of the cyber security attacks, Ransomware attacks have been the most common in the last few years. India witnessed disruptions from cyber attacks through ransomware, Wannacry. These attacks and breaches threaten to trigger heavy damages, including loss of data and disruptions in business. They could also involve regulatory compensation.[8] In India, in May 2017, a data breach at the food delivery App, Zomato, led to personal information of about 17 million users being stolen and put for sale on the Darknet. The company had to negotiate with the hacker in order to get it taken down.[9] In the month of August this year, the police arrested an ex-IIT post -graduate from IIT Kharagpur, Abhinav Srivastava for illegally accessing the server of the Unique Identification Authority of India (UIDAI) through an app named "Aadhaar e-KYC" which was available on the Google Play Store till recently.[10] Some more leakages of Aadhaar data have been in circulation in the news during the last few months.

In the given situation, as discussed above, India needs a comprehensive law on data protection to safeguard an individual's right to privacy. As the Supreme Court noted, this must be achieved by enacting an effective data protection law for India.

Data Protection in India: Present Scenario. The Information Technology Act, 2008: India's existing data privacy framework dates back to 2008, with this being defined under provisions of the Information Technology Amended Act, 2008 (ITAA) under Section 43-A and 72A of the Act.[11]

[8] Economic Times, "Standing Guard at the Gates", Hema Ramakrishnan, dt. 23.9.2017.

[9] The Hindu, "For a safe Cyberspace", Subi Chaturvedi, dt. 19.12.2017.

[10] The Hindu, dt. 4.8.2017.

[11]Sec. 43-A and 72-A of the Information Technology Amended Act,2 008

43-A. Compensation for failure to protect data- where a body corporate, possessing, dealing or handling any sensitive personal data or in information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation:- For the purposes of this section,-"body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(ii) "reasonable security practices and procedures" means practices and procedures designed to protect such information from unauthorised access,damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

(iii) "Sensitive personal data or information"means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

72-A. Punishment for disclosure of information in breach of lawful contract,- Save as otherwise-provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.

Compensation for failure to protect data (Section 43-A) was introduced by way of an amendment in 2008, which states the liability of a body corporate to compensate in case of negligence in maintaining and securing "sensitive data."

Subsequently, IT Rules 2011 were issued by WIPO (World Intellectual Property Organisation) defining in detail the term "sensitive data," something that is lacking in the current Indian legislative framework and the rules governing them. The current legislative framework also fails to mention the case of a breach and the resultant compensation to consumers.[12] In 2014, a bill named The Personal Data Protection Bill, 2014 was introduced in Parliament which has a limited focus. As these provisions are minimal, the legal framework in the shape of contracts under the IndianContract Act, 1872, comes to one's rescue if there is any violation of privacy rights.[13]

Data Protection Law: Initiatives by Lawmakers

(a) **The Parliamentary Standing Committee on Information and Technology:** The Committee chaired by Sri Anurag Thakur, a B.J.P. M.P. Consists of 31 M.Ps from the Lok Sabha and Rajya Sabha. Underlining the need to immediately address issues relating to data protection of government servers, this Parliamentary Panel has identified[14] nearly 20 subjects from four ministries- I&B, Electronics and IT, Communications (Department of Posts) and Communications (Department of Telecommunications). These include problems and challenges including social media oversight to stop terrorism propaganda; oversight of Internet companies such as Facebook, Twitter, Google, for data protection of Indian Consumers.

The Committee will focus on having a government mechanism to evaluate "online terror activities". It will also examine internet companies that gather huge amount of data from Indian citizens in an effort to come up with a system to protect their personal information from getting leaked. One of the focal points of the committee will be online security of data.

(b) **Justice (retd.) B.N. Srikrishna Panel:** In consonance with the Supreme Court's directive in Justice K.S. Puttaswamy's case, the Govt. of India has set up a five member committee chaired by the former Supreme Court Judge, Justice (retd.) B.N. Srikrishna, to draw up a draft Data Protection Bill. The Bill if made law, will be India's first exclusive statute providing protection to online users' personal data from breach by state and non-state players.

The office memorandum of the Srikrishna Committee notes that the "government is cognisant of the growing importance of data protection in India. The need to ensure growth of the digital economy while keeping personal data of citizens secure and protected is of utmost importance."

The recent privacy judgment highlights the Committee's role in evolving a "robust data protection regime." The Court recognised the government's efforts to initiate the process of reviewing the entire area of data protection. It observes that "it would be appropriate to leave the matter for expert determination....."[15]

The new Bill would be based on five salient features: technological neutrality and interoperability with international standards; multi-dimensional privacy; horizontal applicability to state and non-state entities; conformity with privacy principles; and a co-regulatory enforcement regime.[16] This committee is currently engaged in wide-ranging discussions with stakeholders.

Meanwhile, at the behest of Telecom Regulatory Authority of India, India's Telecom Regulator will go in right earnest on data privacy, ownership and security consultations and expects that its

[12] The Indian Express, "Sri Krishna Panel Engaged in Talks with Stakeholders", Sandeep Singh, Anil Sasi, dt.14.09.2017,

[13] Economic Times, "Stringent Data Protection Law is the need of the hour'', O.N. Ravi,dt.15.2.2017,

[14] Economic Times, dt. 9.10.2017

[15] The Hindu, "For a robust data protection regime", Krishnadas Rajagopal, dt. 8.9.2017.

[16] Ibid.

recommendation- likely to be ready in two months- will provide inputs for a government- created committee on data protection. It is hoped that some of the regulator's proposals would assist the Justice B.N. Srikrishna Committee that is identifying key data protection issues in India and recommending ways of addressing them.[17]

Guiding Factors for the New Legislation on Data Protection:

(a) **The Fair Information Practice Principles:**The principles were developed in the 1980s as a response to increased automated use of data, from the bedrock of data protection laws across most jurisdictions. The intention of Fipps is to ensure that even when personal data about an individual is collected, such collection is lawful, and the individual contains to be able to exercise control over it.[18]

Fipps prescribe the following minimum standards of data protection:

1. Personal data must be collected with the consent of the individual, (ii) Its use must be limited to the purpose of collection; (iii) the individual must continue to have access to her personal data and be able to rectify it; (iv) the data must be accurate; (iv) and organisations must ensure data- security measures to protect personal data.[19]

While India does not have a data protection statute, the Information Technology (Reasonable Security) Practices and Sensitive Personal Data or Information) Rules, 2011, issued under the I.T. Act, seeks to introduce Fipps in India. While the rules are a first attempt towards framing a legal framework for data protection, they fall considerably short of internationally accepted data-protection standards.[20]

First, they apply to a restricted category of data that are deemed 'sensitive' in nature. This includes data such as those pertaining to physical, physiological and mental health conditions, sexual orientation, medical records, biometric information, etc.[21]

Second, they apply only to the private sector, thus, giving the government a free reign to collect and use people's personal information as their discretion. Further, it allows for unlimited sharing of data with the GOI on broad grounds such as prevention, detection, investigation including of cyber incidents, prosecution and punishment of offences, etc., coupled with a limited obligation on the government to not disclose such data.[22]

Finally, the absence of an independent and effective enforcement mechanism means that these rules are nothing but a paper tiger.[23]

Other than IT rules, scattered instruments across sectors such as circulars issued by the Reserve Bank of India requiring the formulation of privacy policies, the Credit Information Companies (Regulation) Act, 2005, and allied rules, and provisions of licensing agreements for telecom service providers recognise limited Fipps. However, they too fall short.[24]

(b) **Report of the Group of Experts on Privacy, 2012:**[25] Headed by the former Delhi High Court Chief Justice A.P. Shah, it was constituted by the erstwhile Planning Commission. Both the government and the Court have agreed that this would be the "conceptual foundation for legislation protecting privacy" in the form of the new Data Protection Bill.[26]

---

[17] Economic Times, dt. 1.9.2017.

[18] Economic Times, "Saving Privacy for Public Good", Akriti Gaur & Namrata Mukherjee dt. 15.9.2017.

[19] Economic Times, "Saving Privacy for Public Good", Akriti Gaur & Namrata Mukherjee dt. 15.9.2017.

[20] Ibid.

[21] Ibid.

[22] Ibid.

[23] Ibid.

[24] Ibid.

[25] Rishika Taneja, Sidhant Kumar, Privacy Law, Appendix 4,Eastern Book Company, Lucknow, 2014.

[26] The Hindu, "For a robust data protection regime, Krishnadas Rajagopal, dt. 8.9.2017.

The Justice Shah Group had emphasised on taking the informed and individual consent of users before the collection of their personal data. It had proposed giving users prior notice of information practices, providing them with choices, and collection of only limited data necessary for the purpose for which it is collected. If there is a change of purpose, it must be notified to the individual.

Most importantly, the report proposed access for users to their personal information held by a data controller. Users should be able to seek correction, amendments, or deletion of inaccurate information.[27]

(c) **European Union's General Data Protection Regulation**: India needs a separate law on privacy and data protection, ideally on the lines of the said regulation adopted in 2016 and slated to come into force in May 2018.[28] The European Commission in January 2012, proposed a comprehensive reform of data protection rules in E.U. that aim to give back to citizens' control over their personal data, and to simplify the regulatory environment for business.

Beyond the potent Data Protection Law: Some points to Ponder

1. In India, we still lack a proper and Art of the State data storage infrastructure, mainly building safe from outside intrusion and the necessary furnishings etc. Our existing system is basically founded on the colonial British system for keeping records which we have inherited. Indeed, that system has outlived its utility and we have to build a new system based on the best practices of European Union, American and other western countries. Keeping computers, servers and the other necessary documents requires a well thought out system of upkeep. Their security is also of paramount importance.
2. The man- management of such institutions or places of data storage should be well planned and the role of every individual officer- bearer should be clearly spelt out. Otherwise, when something goes wrong in our official establishments, the pinpointing of the fault becomes almost an impossible tasks. The staff appointed must be well trained also for their assigned jobs.
3. Human element is of utmost importance as regard to selection of personnel for data collection centres. Men of proven integrity and commitment should be assigned definite roles in such places. Otherwise, leakage of data can't be ruled-out.
4. At present, nearly all the social networking sites have their head-quarters in the U.S.A. and the whole data is under their control. In times of crisis, even the governments beg for data from these sites. This dependence is not healthy for data protection regime in India. Our software engineers and other technical persons should strive to develop our own servers and websites so that the data of the citizens of India may remain within the control of our people. This is also necessary in the light of Snowden's revelations regarding probable misuse of data of foreign countries by the U.S.A. through the Prism Project. National Security should be the foremost concern for all of us.
5. In this age of Artificial Intelligence, we can also think of taking recourse to it in the maintenances and upkeep of the huge stored data.
6. Lastly, unless we develop a strong battery of experts, the menace of hacking can't be countered. India has vast potential of software and computer experts who can be motivated and trained for anti-hacking activities.

In short, we need a holistic approach towards the task of data protection. Mere a comprehensive law in this regard will not suffice.

Conclusion

In this digital era, a robust legislative framework for data protection is urgently needed in Indian context. As far as government's view is concerned, the proposed law would walk the "fine

[27] Ibid.

[28] Economic Times, Editorial, dt. 15.9.2017.

balance" between the need to respect data sovereignty of Indians, their data should be made available also for legitimate concerns, legitimate interest and for development of India. However, the balance between innovation and privacy must lean towards people's rights, and not the industry. There must be specific protection for the individual against unjustified, and not merely unauthorised, snooping by government agencies. Any breach of privacy must be authorised by a court order and the agency responsible must be held to account by a committee of parliament, and not merely by the executive. We need a law to create data protection and a regulator who would be accountable for the job. Any law on data protection must be within the framework of the Indian Constitution respecting people's rights. Data protection is not about protecting data, it is about protecting people.

Bibliography

1. Aulak, Gulveen; Trai to go full throttle on Data Privacy, Economic Times, dt. 1.9.2017.
2. Chaturvedi, Subi; For a safe Cyberspace, The Hindu, dt. 19.12.2017.
3. Gaur, Akriti & Namrata Mukherjee; Saving Privacy for Public Good, Economic Times, dt. 15.9.2017.
4. Rajagopal, Krishnadas; For a robust data protection regime, The Hindu, dt. 8.9.2017.
5. Ramchandran, Hema; Standing Guards at the Gates, Economic Times, dt. 23.9.2017.
6. Ravi, O.N.; Stringent Data Protection Law is the Need of the Hour, Economic Times, dt. 15.2.2017.
7. Singh, Sandeep & Anil Sasi; Srikrishna Panel Engaged in Talks with Stakeholders, The Indian Express, dt. 14.9.2017.
8. Taneja, Rishika, Sidhant Kumar; Privacy Law, Eastern Book Company, Lucknow, 2014.
9. The Indian Express, dt. 10.9.2017.
10. Economic Times, dt. 15.9.2017.
11. Economic Times, dt. 9.10.2017.
12. The Indian Express, dt. 30.8.2017.