International Journal of Modern Agriculture, Volume 10, No.2, 2021
ISSN: 2305-7246

A STUDY OF THE LAW REFORMS NEEDED IN THE DATA PROTECTION LAW OF INDIA

Dhrumi Gada[1], Santosh Aghav[2]

[1]Symbiosis Law School, Pune
[2]Symbiosis International (Deemed University), Pune, India
*Email: [2]saghav@symlaw.ac.in

Abstract

Presently, in our country there is no legislation that has been passed for protection of personal information or personal data collected by various institutions and organisations. It is a run of the mill now, that an individual's data is collected for purpose A, but then is used for purpose B which has not been consented by the individual from whom the data is collected. Many a times this data is even sold to various organizations in return for a monetary benefit, and then this data is used by the companies who have purchased it, to further their marketing base and approach customers to outdo other organisations in their business.

Also, not only for targeting customer to enrich their marketing base, but data of individuals is also collected to completely monitor and stalk their various activities such as daily surfing, the things they like, shopping sites they use, which web pages they frequently visit, or which religion do they follow or which political party are they inclined to, as in the Cambridge Analytica case. This information is used for various dark uses, which the customer cannot even think of.

This whole aspect of data protection circulates around the right to privacy of an individual, which is guaranteed under the constitution. Accordingly, various provision of the draft bill of the Personal Data Protection Bill, 2019 have been discussed below and reforms have been suggested for the same. This is a research paper conducting a law reform research in the context of the current Indian legal scenario on personal data protection of individuals..

Key words: data protection, right to privacy, data breach, data collection, principal, processor, fiduciary, data subject, consent, law reforms, bill, recommendations, loopholes

Introduction

Data is enveloped around us and is generated in virtually every action we do and anything we engage in. On one side, there is data, which we may allow to be shared voluntarily and give consent for it to be collected, and the second type is the data, which is produced at every minute when we do something, and which we are not interested to share. And this is the data that is priceless and a plethora of organisations, institutions as well as companies are willing to pay billions and trillions for it. What is extremely surprising is that people are unknown of the value of the data they are intending to purchase and the maximum potential that data can have and the ripples it can create within an economy. With the progress of technology, newer applications are born enhancing the value of the data.

Data breaches and leaks in the world have risen to another level. In this digital age, of virtually and universally open access to the Internet, let's just say that data is the new oil. Let's just say that data is the new currency. In earlier times, people used to even resort to illegal things to earn a buck but now, people, businesses and organizations can actually do anything to get access to such data.

Several questions have now emerged in the limelight: Whom does this data belong to? What exactly are data subjects? In what form is their consent collected? Who does the data go to? Where all can a person's data travel? Who has the permission to access this data? Are all the terms and further uses disclosed to them while collecting their data? What are the limitations on the use, manipulation, re-sharing and exploitation of this data? Several government bodies are also wanting access to data from their own citizens, businesses, industry players and large corporates, which further complicate this position. On the other side of it, what are the kinds of limits

to infringement of privacy? What exactly does data protection mean in terms of privacy of an individual? Can unnecessary demands of data be made by the government bodies under the pretext or for reasons of government benefits or services? Should security as well as the interest of the nation surpass all the privacy concerns?

Legislators, judiciary and the law enforcement all around the globe are yet struggling really hard to marry traditional concepts and provisions of the law of the law, when it comes to data and several questions around its periphery.

Presently, in our country there is no legislation that has been passed for protection of personal information or personal data collected by various institutions and organisations. It is a run of the mill now, that an individual's data is collected for purpose A, but then is used for purpose B which has not been consented by the individual from whom the data is collected. Many a times this data is even sold to various organizations in return for a monetary benefit, and then this data is used by the companies who have purchased it, to further their marketing base and approach customers to outdo other organisations in their business.

Also, not only for targeting customer to enrich their marketing base, but data of individuals is also collected to completely monitor and stalk their various activities such as daily surfing, the things they like, shopping sites they use, which web pages they frequently visit, or which religion do they follow or which political party are they inclined to, as in the Cambridge Analytica case. This information is used for various dark uses, which the customer cannot even think of.

This whole aspect of data protection circulates around the right to privacy of an individual, which is guaranteed under the constitution. Accordingly, various provision of the draft bill of the Personal Data Protection Bill, 2019 have been discussed below and reforms have been suggested for the same.

Reforms In The Personal Data Protection Bill: The Need Of The Hour

India is yet ill-equipped to deal with emerging threats related to data protection as India still continues its policy of reactive responses rather than proactive measures. The various issues and concerns highlighted below mandate the urgent need for a fast rethink and reforms in the current legislative scenario of India with respect to the current landscape of data protection in the country. Below are some of the reforms that are needed in the Personal Data Protection Bill, 2019.

(i) The definition of 'personal data' is really wide in the bill. **Section 3 (29)** of the Bill 2018 says: "*"Personal data" means data about or* ***relating to*** *a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information.*" The above-mentioned wide definition could result in denial of information or collection of personal data even if it is not exactly data that could help personally identify someone but if it is just relating to a natural person. Thus, the ambit of rejection is expanded without bounds since, the scope of this definition and the content it envelops it is virtually unlimited.

(ii) In **Section 43 (1),** the draft bill mentions the following: "***Processing of personal data*** *in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of law* ***shall not be permitted unless it is authorized by a law made by Parliament and State Legislature and is necessary for, and proportionate to, such interests being achieved****."* Incase an LEA wants to collect and process personal data of any accused or suspects, for the enforcement of the law prevalent in the state, then this provision will make it difficult for them, unless there is a law already in place or otherwise a law is passed by the Parliament or the State Legislature.

Thus its not right, that the mode, manner and process by which LEAs therefore may undertake data processing is now left to "law, made by Parliament". Such law further has to be "proportionate to, such interests being achieved", which is not clearly outlined in the Act.

(iii) In **Section 43 (4),** the draft bill mentions the following: "Personal data processed under sub-section (1) **shall not be retained** once the purpose of prevention, detection, investigation or prosecution of any offence or other contravention of law is complete **except** where such personal data is necessary for the maintenance of any record or database ***which constitutes a proportionate measure to prevent, detect or investigate or prosecute any offence*** or class of offences in future." Here, there is no clarity whether what records of personal data would constitute a 'proportionate measure' to prevent, detect, investigate or prosecute any offence or class of offences in future, which again gives excessive power in the hands of the government without any particular guidelines for it to be used.

Thus, the degree of proportionality should be defined to an extent, which would reduce the burden of litigation filed in the courts. Also, in preliminary enquiries and for crime prevention, LEAs generally need more information since there is limited evidence about the suspect until this stage, thus retention of personal data would become a problem cause of this section, as investigation at this stage involves having expansionary searches, scraping, etc. across a lot of information. In cases involving intelligence and counter-espionage, this need of retention of data is even furthered.

(iv) The Bill imposes "***liability on the directors of a company or the officers in charge for the conduct of the business of the company at the time of commission of the offence***." This comes off as a very harsh measure, which takes a very extreme stand, as even most international legislations such as the GDPR do not provide, in the case of breach of data, for liability of the person responsible for the conduct of business. Further, due to no specific clarity on the side of the law, the officers in-charge as well as the directors, may be held liable to pay the same amount of penalties as may be imposed on the company, which again proves to be unfair.

Restrictions under S.42 & 43, the LEAs believe, are excessive and onerous. They agree and accept the need for the limitations pertaining to regulation of data processing to be necessary and proportionate for achieving purpose. However, LEAs believe that the threshold of compliance needed for LEAs appear to be in excess of those imposed for instance on Journalists under S.47, where under the only compliance mandated is compliance with "Code of Ethics" issued by the Press Council of India or other "self-regulatory" organization.

(iv) There again is clarity lacking ***on the nature of liability imposed interse between a data processor and a data fiduciary, or between other various data processors in case of breach data***. So, if the data is shared with the data fiduciary which then determines how the data is supposed to be processed by the data processor, and in turn if the data is shared with any other third party, the liabilities which can be imposed on the third parties to whom the data is shared by the data processor, the right to erasure of data of the data subjects, the data retention period which they have to abide by, whether consent of the data subject has to be taken and in what form, all this is a bleak concept, undefined by the bill as of now.

(v) There is no such timeline in the law to define a particular period in which the data protection officers shall reply. Thus, the ***Data Protection Officer, mandated by the law, must be made to reply in a time-bound manner*** say a week or two, failing which the Data Fiduciary must be made to face legal action. Also it is feasible, if a Law Enforcement Agencies especially, the time must be bound up to seven days. This is crucial because such sources of information are crucial for investigation of cases.

Also in an ***interview with Mr. Balsing Rajput, the Superintendent of Police at Maharashtra Cyber***, he mentioned that, 'Facebook, Twitter, SBI, Instagram, TikTok, Telecom operators and other intermediaries are pretty reluctant to give out personal data and there is no person to oversee the time they take to process such personal data of accused or suspects that we ask for while investigating our cases. Thus there should be an authority and a timeline should be in place for the cases to be solved and information to be processes as we, the law enforcement agencies need quick processing of personal data to move ahead in investigations or else many a times the evidence is just lost.'

Thus, there is a requirement of strong provisions for enabling LEAs to call for records / documents from Intermediaries, to facilitate investigations; and for sanctions against entities for non – compliance, including for providing specific time bound replies;

(vi) Also, surveillance of data subjects by the state is covered in the bill but**, *surveillance by Non-State Actors*** must be expressly dealt with by the Bill as many surveillance activities in the past have been

(vii) ***Combating fake news***: There are already serious repercussions due to fake news and Government is contemplating special laws to curb the menace. In such instances, it is imperative that such persons or entities ought to:

1. Have similar restrictions on necessity and proportionality be applied for journalistic data processing;

2. Mandate regulation by a Government authority or parliamentary laws, which will ensure due compliance; and

3. Provide for legal remedies against fake news and unethical or immoral journalistic practices including against paid news.

(viii) ***Data localization feasibility:*** While the new draft has relaxed the need of localization or storing a mirror copy of personal data processed by companies outside India on a local India server or data center which is located in India, ***the rules regarding localization of sensitive personal data is still the same.***

Thus, ease of doing business for companies that are based out of India, but process a lot of information in India, which is Sensitive Personal Data (SPD), has been made difficult. The companies will face a lot of costs for setting up servers, hosting the data locally of millions of users and adhering to the transition, due to which it could be possible they these companies stop dealing with Indian residents, thus affecting the revenue of India.

(ix) ***Investigation of such cases by a Police Inspector:*** The real concern in this Chapter is with respect to vesting the investigation powers only with a police officer of the rank of not less than an inspector. Data protection is to apply to all equally including those in remote or rural areas. It is a matter of fact that in many instances, ***there are not even Assistant Police Inspectors in several police stations in remote or rural areas***. Such rigid rules for investigation will negate the effectiveness of the proposed enactment. ***Victims will be the ultimate sufferers.***

Prosecutions also get weakened when a senior police officer is burdened with investigations under special laws including the IT Act. The intent behind this is understandable i.e., that a police officer of lower rank may not be knowledgeable in the intricacies of such special laws or that the provisions may otherwise be abused. However, and in the light of ensuring actual and effective implementation of the provisions, it is important that S.94 be reviewed to allow police officers of lower rank to also undertake investigations.

Thus, Police officers of rank, lower than Police Inspector to also be allowed to undertake investigations under the proposed data protection enactment; In the alternative, S.94 to be revised to only indicate that where possible, the Inspector of Police will undertake or oversee investigations under the data protection enactment; To balance both requirements, investigative powers may be modified to oversight by the senior-most station house officer of the police station, in investigations under the data protection enactment.

(x) ***Classification of Intermediaries***: Firstly, an intermediary's role is limited to just providing a platform for its users to publish or post content and data and take the benefit of its services. It should not play a role in deciding what content is supposed to be published and what services would be availed. Secondly they have a major role to keep their platforms aloof from unlawful content being posted online. But if, an intermediary from a passive platform becomes an active one, to determine the reach of content and ranking, then the shield of 'safe-harbor' protection is removed and a lot of penalties and sanctions can be attracted.

The bill has just provided for classification of intermediaries as 'Social Media Intermediaries', but no such classification of intermediaries is done on a function based approach as to how much of the content they host and how much of it they manipulate or control which actually attract the data protection provisions. The rules and guidelines on the intermediaries shall be applied according to the function they deliver or operate on. These rules shall have a function-based approach, and should be regulated according to the different functions they play on the Internet.

(xi***) No clarity on the definition of 'Critical Personal Data'***: data as been categorized as Personal Data, Sensitive Personal Data and Critical Personal data under the bill. Thus, Clarification is sought on the definition of "Critical personal data" under the Draft Bill as the definition and the ambit of it may vary on a case-to-case basis. To avoid further accumulation of litigation and unnecessary filing of cases for breach of critical personal data a clear line needs opt be drawn within these three sets of data, and it cannot be left at the whims and fancies of the judiciary to decide and interpret every time differently according to the case that is in front of them. Pre-defined criteria for data to fall under one of these three categories, will make the data subject aware of the what data has been infringed and will also make the data processor aware of what consequences they can face according to the breach of which set of data that has occurred.

(xii) The Right to be forgotten and the right to erasure / delist concept: The right to be forgotten aspect in India, is still an evolving domain and is yet to be explored unlike the western countries. We do have the Personal Data protection Bill, 2018, and the right to be forgotten clause, but the Indian law does not really distinguish or give the option as to when to exercise the right to erasure and the right to delist. Right to erasure may mean complete deletion of records from the history of Internet. This right may be exercised as in the case of a criminal case against someone who was later acquitted, but the name still appears on the web that he was tried in the court for this case, which may affects his employment opportunities as well as his reputation [Laksh Vir Singh Yadav v. Union of India & Ors. 2016 W.P. (C) 1021]. Whereas right to delist may mean that the search engines may be prohibited to show the same in the search results, but someone who may have the original link of the article can always access it. India's Draft Personal Data Protection Bill, 2018 does mention for a right to be forgotten, which entails and gives power to an individual the right to restrict or stop the information form being disclosed, but does not in the literal sense mean a right of erasure, which may be important for protection of minors, reputation damage in criminal cases or insolvency proceedings.

Also there is no provision, unlike in the General Data Protection Regulations (GDPR), if along with a main data controller there are various other data controllers handling your information or if a particular intermediary outsources the complete data management aspect to another company. What happens in this situation, if you no longer want to use the services and ask the data controller to delete all the information regarding you? Are there any clause that makes sure that not only the main controller but all the other entities possessing your data are also faced with the same data deletion obligations?

Also, under the GDPR, a data principal himself or herself can ask the data controller or the data processor to go ahead and remove or erase his/her data and if they refuse, then the principal can approach the supervisory authority [Supervisory Authority is an independent public authority, which is established by each member state of European Union for monitoring the application of GDPR under Article 51 of GDPR]. But in the Indian PDP bill, the data subject has to first approach an adjudicating officer for exercising his / her right to be forgotten, which makes the whole process futile and time consuming and the damage done could also be grave, if the data is not forgotten or erased in a timely fashion. Surprisingly, this section also gives, any other person the right to challenge the order of the adjudicating officer granting the right to be forgotten. Thus, the real question is whether who owns the personal data and whom should it concern? Can any other person, who does not really own the data, be allowed to challenge a right to be forgotten order in respect of the data that is owned by someone else?

(xiii) ***The Lack of classification of Intermediaries with respect to the data collection powers they possess:*** Many countries like the EU, Australia and Singapore have classified intermediaries according to the functions they perform and the degree of liability is also concurrent to an extent similar to the function and the level of control they have over the content that is hosted on their platforms. For example, if the intermediary platform does host user-generated content but has modification rights like initiation, selection of receiver as well as modification of content then the safe harbour protection is not usually granted to the intermediary. Online marketplaces like Flipkart, Myntra, Amazon, Google, which actually show us search results according to our inferences and collect data when we surf on such platforms does not make them mere conduits but more like moderators. Google itself says that, "When you're not signed in to a Google Account, we store the information we collect with unique identifiers tied to the browser, application, or device you're using. This helps us do

things like maintain your language preferences across browsing sessions", does it really just make them mere transmitters or platforms for hosting content or they are as smart as robots to understand the what content to show, what data to collet and what change ins services to be offered according to the change in demography and preferences of an individual.

The theory of proportionality should be applied wherein the liability should be proportionate to the control that the platform has over the content to be hosted over it. Platforms like Zomato, Swiggy, Uber, Ola are not same for all, as everyone gets coupon codes, offers, discounts that differ from time to time upon their usage of the app and how often they use their services. If I book a cab to a same location and if someone else who stays next door also books a cab to the same location, there are higher chances for me to get a cab if I have good rating as a traveller in my past rides from the drivers I travelled with and travel very often, even if the other person is shown unavailability of cabs due to bad ratings or lesser usage of the app.

Thus where modification is done to a very minimal extent on the content produced in the platform, then such intermediaries can be extended the concept of immunity and safe harbour protection provided they follow certain due diligence measures.

The next category could be the telecom companies, the domain name servers, web hosting platforms and cyber café that are mere conduits and play no role in modification of content and all the users are treated the same with no change of content hosted by it, Thus, these all fall under complete and unconditional immunity from being liable.

Thus, these are some of the major reforms needed in the bill that is currently under the review with the Joint-Committee of the parliament.

Conclusion

Data protection issues have cropped up time and again and have also raised an alarm with the authorities about various issues such as privacy, misuse of data, confidentiality, right to be forgotten and right to erasure, national security, cyber extortions and various other issues. With the more and more diversion of people from offline to online platforms and intensive engagement of people in activities like e-shopping, e-commerce, online payments and internet banking, it is of the utmost need that the loopholes are plugged in the current draft bill that is pending for approval.

There is a greater need for all the big tech giants, academic professional as well as the society to come together and ensure that they develop guidelines or frame such policies in this world of digitization wherein rights of users are not compromised and a balance is struck between the right of the users such as the right to privacy and the liability of the data processors and controllers. Being one of the hot topics of discussion, with even the non-personal data structure being discussed for India, legislatures are required to make sure the steps are taken in the right direction, in a qualitative and effective manner.

Law and technology were never on good terms with each other and the law has never been at par to tackle the nuances posed by the technology, which are rapidly evolving. This is because, the law has always been lethargic to respond to various challenges posed by technology every now and then. Despite the efforts of the legislature to draft a personal data protection bill, the legislation has left various lacunas, which need to be redressed via reforms, and rethinking the bill again, which may introduce changes for the better.

References

1. The Personal Data Protection Bill, 2019

2. The General Data Protection Regulation, European Union

3. Information Technology Act, 2000 along with its amendments

4. Information Technology (Procedure and safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009

5. Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

6. The Information Technology (Intermediaries Guidelines) Rules, 2011

7. Arthur T. von Mehren and Donald T. Trautman, Jurisdiction to Adjudicate: A Suggested Analysis, 79(6) Harvard Law Review (1966) at p. 1126

8. Andrew Keane Woods, Against Data Exceptionalism, 68 Stanford Law Review (2016) at pp. 765-773

9. Anupam Chander and Uyên P. Lê , Data Nationalism, 64 Emory Law Journal (2015).

10. Christopher Kuner, Data Protection Law and International Jurisdiction on the Internet (Part 1), 18(2) International Journal of Law and Information Technology (2010) at p. 20.

11. Edward J. Bloustein, Privacy as an Aspect of Human Dignity- An Answer to Dean Prosser (New York University, School of Law, 1964).

12. Girish Ramchandra, Data Protection and the Legitimate Interest of Data Controllers, Common Market Law Review (2014)

13. Haresh Maniar, Privacy as Contextual Integrity, NULJ Law Review (2004)

14. Jack Goldsmith, Unilateral Regulation of the Internet: A modest defence, 11(1) European Journal of International Law (2000) at p. 139

15. Joshua Mahajan and Christoph Engel, Privacy as a Public Good, 65(3) Duke Law Journal (2015) at p. 396.

16. Michael J. Kelly and David Satola, The Right to be Forgotten, University of Illinois Law Review (2017) at p. 1.

17. Nancy King and Jay Mehta, Data analytics and consumer profiling Finding appropriate privacy principles for discovered data, 32(5) Computer Law and Security Review (2016) at pp. 699-700.

18. Neil M. Richards, The Dangers of Surveillance, 126 Harvard Law Review (2013) at p. 1939

19. O. Tene and J. Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11(5) Northwestern Journal of Technology and Intellectual Property (2013) at p. 242.

20. Paul Ohm, Broken Promises of Privacy: Responding to the surprising failure of Anonymisation, 57 UCLA Law Review (2010) at pp. 1717 to 1722

21. Polonetsky, Tene and Finch, Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification, 56 Santa Clara Law Review (2016) at p. 619.

22. Rishabh Dara, Intermediary Liability in India: Chilling Effects on Free Expression on the Internet, The Centre for Internet & Society (2011)

23. Shalini S., Era of Online Criminal Conduct, CCG Working Paper Series No. 2 (2015-16).

24. Sheri Vora and Tanisha Naik, Web Sites for Young Children: Gateway to Online Social Networking?, Professional School Counselling (2009)

25. Shripati Acharya, The great Indian data rush, Yourstory (26 February 2018)

26. Tatevik Sargsyan, Data Localisation and the Role of Infrastructure for Surveillance, Privacy, and Security, 10 International Journal of Communication (2016).

27. M. Kaul, (March 13, 2013), India has an internet problem, Open Democracy