International Journal of Leading Research Publication (IJLRP)
E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

Dusk before the Dawn? Critical Analysis of the New Data Protection Law

Dr. Rishu Dev Bansal

Principal, Seth G.L. Bihani S.D. Law P.G. College,
Sri Ganganagar, Rajasthan

Abstract

It is often said that Data is the new oil. With an intensely digitalized world and an increasingly digitalized India, the significance assumed by the data has reached unprecedented heights in the last couple of decades. The motive behind most of the cyber security attacks in India in the recent past has been aimed at stealing data. There have been numerous instances of health data, financial data and other important personal and sensitive data being compromised by the cyber attackers. Numerous instances of data breaches including the hacking of social media accounts 6, theft of credit and debit card details and other privacy breaches go unreported due to the lack of stringent data protection laws in India that could afford adequate protection to the sensitive and personal data of the citizens in the recent past. This Study has been taken up with the specific objective of studying the existing and upcoming data protection law in India while comparing it with the laws in advanced data protection regimes in order to highlight the lacunas in our data protection framework. The law of data protection is of particular concern to India due to innumerable factors, the most prominent of them being the extensively vast population of India. India has over 500 million Internet users and the count growing at a rate of over 8% per annum; it is by far the biggest market in the digital economy as of today. With the digital economy in India headed towards an unprecedented boom, it may soon become a very impending challenge to address the issues arising out of voluminous transactions in the form of the digital medium.

Keywords: Data Protection Law, Privacy Legislation, Digital Privacy, Data Security, Data Privacy Rights, Data Breach Laws

Introduction

The relationship between technology and humanity has existed since humans first walked the earth's surface. People appreciate their own space and liberties. They have an inquisitive mind, therefore they are constantly looking for better ways to do tasks. Human curiosity unraveled the insider facts of nature, resulting in a perpetual flow of innovations. Today, the primary thrust of innovation is toward technical advancements, which have brought new concerns to our privacy and the security of global information infrastructure. One of the most recent needs of modern civilization is for the finest method to manage the vast amount of information produced by modern living Privacy is an essential value for development of human personality. In earlier times man used to possess personal property i.e. his land

and house. Therefore, the privacy was related to personal property of him.[1] Threat to his privacy was from government which has power of search and seizure and from private persons who trespass the property. However, with advancements in science and technology, people's lives have come under continual societal scrutiny. Particularly social media and online service platforms and Mobile Apps, has also contributed to an individual's invasion of privacy. Individual personal information is given to society that was not meant to be disclosed. In general, a person wishes to have control over the dissemination of his personal information. People have become oblivious to the dangers of using IT services based on Artificial Intelligence.

Today, A.I based sophisticated devices, particularly wearable gadgets, have crushed 'privacy' to its core, and personal information has become a 'commodity' as a result. It's now for sale. With the increased usage of information technology and computers, service providers acquire information on an individual. This personal information is being used unlawfully for commercial gain. As a result, an individual's privacy is jeopardised, infringed upon, and violated. Persons' informational privacy is being violated in the present age of information revolution. The consequences of this invasion may include the loss of legal and human rights.[2] It is a matter of consideration that how technological changes have affected scope of legalprovisions. The protection provided under the legal provision soon become insufficient due to technical change advancing character or use of technology. Many times the scope of existing protection under law is narrowed down by progressive technological changes.[3]

In modern era, impact of advanced technology on law is unprecedented It is essential to know the threat for protection from the threat. To control and/or regulate such misuse or abuse, the legal provisions are enacted by different legal systems. To protect the Right to Privacy, European Union has enacted different privacy laws which also covering Artificial Intelligence related privacy breach issues.[4]

In the recent past, India has also witnessed a fillip in the use of digital space in the sector of finance and with an influx of more advanced technologies and an aggressive posture from the government to promote digital transactions after the demonetization, has made the use of data even more significant and prone to misuse at the same time. The growth in usage of online platforms like Google Pay, BHIM, Paytm and numerous other start-ups facilitating digital transactions are testimony to the fact that the Indians have entered into an age where these digital mediums have become an indispensable aspect of our lives and thus there needs to be a strong and effective mechanism in place in order to provide adequate security to these transactions. With the penetration of high-speed Internet within the nooks and corners of the country, the threat to the informational privacy looms larger than ever now. While the digitalization of the economy has opened the way for a plethora of job opportunities in the sectors pertaining to Health, Education and Governance, the need to have a strong law in place in order to ensure maximum protection to these personally sensitive data of the individuals becomes more

[1]Addison Litton. The state of surveillance in India: The Central Monitoring System's chilling effect on self- expression. Wash U Global Stud L Rev. 2015;14:799- 720.
[2]Information Technology Act, 2000. No. 21. Acts of Parliament; c2000. India.
[3]IT (Amendment) Act, 2008. No. 10. Acts of Parliament; c2009. India.
[4]The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. No. 18. Acts of Parliament; c2016. India.

important than ever.[5]

The most important aspect of the research was aimed at critically analyzing the provisions of the proposed data protection Act and thus to come to arrive at the answer to the hypothesis of the thesis. After, a detailed discussion into some of the key aspects of the proposed law, the researcher has come to the conclusion that the hypothesis of the research stands answered in positive, an outcome that was more or less apparent from the discussions in all the chapters.[6] It is without doubt, true that the Personal Data Protection Act, 2023 fails to address some of the most pressing issues concerning the data protection laws in a free democratic society.

Need For A Broader Scope Of Data Protection

The preamble of any legislation is one of the most vital factors influencing its interpretation by the judiciary. Thus, it becomes optimal to have a preamble that is precise and assertive about its object. The Data Protection Act's prime objective should be guaranteeing the right to data privacy of the citizens of India and fostering a data protection regime that is sensitive to the remotest of the breaches to the right to privacy.[7] The preamble must also incorporate within its fold an unequivocal commitment from the government against illegal intrusion in the private realm of the individuals with a detailed roadmap of surveillance reform. The preamble should also take into the account the pressing need for creating awareness within the country about the contours of right to privacy and thus felicitate a privacy conscious society. It is proposed that the preamble be amended as: The preamble that in pith and substance incorporates these objectives will provide a greater width to the rights recognized in the legislation. It is submitted that the aspects like fostering a digital economy andundue emphasis on the economic aspects of data shall do no service to the right to privacy. While, these objectives may be ancillary to a robust data protection regime, the rights to privacy must not be pushed to the backseat on the premise of fostering digital economy. The preamble must "call a spade a spade" and recognize the pressing need for the surveillance reform in the country and lay down a vision for a regime that is truly protective of the right to privacy in the long run.[8] The preamble must in unequivocal terms endorse the constitutional necessity of protecting and preserving the fundamental right to privacy and thus a need for setting up a truly independent body to enforce it.

The second most important aspect of any data protection legislation, after the preamble, is its scope. This means to say that the extent of application of the legislation determines its effectiveness in meeting its objectives set out in the preamble of the legislation. The proposed Act omits the non-personal data and the anonymised data from the application of the provisions of the law. It is submitted that numerous real-life cases have established the fact that even the non-personal data and the anonymised data can be combined to form the personally identifiable information. In the age of Big Data analytics, where the data can be collected in the form of meta data which can further be processed as the

[5]Chander A, Land M. United Nations General Assembly Resolution on the Right to Privacy in the Digital Age. Int'l Legal Mater. 2014;53:727-735.
[6]Wankhede A. Data protection in India and the EU: Insights in recent trends and issues in the protection of personal data. Eur. Data Prot. L Rev. 2016;2:70-73.
[7]Duraiswami DR. Privacy and data protection in India. J Law Cyber Warfare. 2017;6:166-169.
[8]Ramnath K. ADM Jabalpur's antecedents: Political emergencies, civil liberties, and arguments from colonial continuities in India. Am U Int'l L Rev. 2016;31:209- 225.

personally identifiable information, such wide exemptions to the non- personal data may prove to be fatal to the prospects of the data protection regime in the country.

While it is true that the data anonymisation may substantially reduce the risk involved in processing of data but the possibility of reversibility of the process cannot be ruled out altogether.[9]

A restricted definition for categorizing the data as anonymised data will substantially reduce the volume of data which might be designated as non-personal. It is also suggested that the provision of the Act proposing the sharing of the non-personal data with the central government ought to be omitted altogether. It is often pointed out that the provisions providing for the "Promotion of Digital Economy" be duly omitted.[10] As previously proposed, the objective of promotion of the digital economy is not in consonance of a robust data protection regime and any emphasis on the aspect may be used by the Central government to seek huge volumes of potentially personally identifiable data on the pretext of promoting a digital economy. The evidence of such attempts is amply reflected in the Section 91 of the proposed Act. It is pointed out that the language of the section 91 is a reflection of a colorable attempt from the Central government to compel the Data Protection Authority to share the "Non-personal" data for all practical purposes.[11] The provision also asserts in no uncertain terms that the decision of the central government upon the determinative question on sharing of such data would be final.

It ought to be pointed out that none of the progressive data protection regimes across the world contain such blanket assertions enabling the State to process any personal data, covered under the guise of non-personal data for the purposes of policy making and better targeting of the welfare schemes and the retention of the aforementioned provisions in the final Act shall be detrimental to the very concept of a robust data protection regime in the country.[12]

A Feeble Data Protection Authority

The data protection authority is the cornerstone of any data protection authority all over the world. One may hold theposition of data protection authority in a digital society to be analogous to the election commission in a democratic society. What India, as a country which is yet at a nascent stage of its awakening as a privacy conscious nation, needed was an independent agency that would place the interests of the data principals as the most sole objective of its existence? The data protection authority is not just a statutory body that should act upon the whims and fancies of the government of the day, instead the real objective behind having a data protection authority is to have an autonomous agency in place that would afford sufficient safeguards to the citizens against any attempts from the part of the state to infringe the right to privacy of the citizens. In what comes as the most unfortunate and disappointing aspect of the proposed data protection Act is the office of the Data Protection Authority. What the Act envisages is not a data protection authority even in the remotest sense. The proposed authority is just an extension of the central government with no element of independence and accountability mechanisms in place. The following are some of the most crucial aspects of the data

[9]Singh S. Privacy and data protection in India: A critical assessment. JILI. 2020;110:53-57.
[10]Basu S. Policy-making, technology and privacy in India. Indian J Law Technol. 2010;6:65-70.
[11]Determann L, Gupta C. India's Personal Data Protection Act, 2018: Comparison with the General Data Protection Regulation and the California Consumer Privacy Act of 2018. Berkeley J Int'l Law. 2019;37:481-501.
[12]Nilekani N. Data to the people: India's inclusive internet. Foreign Aff. 2018;97:19-33.

protection authority that the proposed Act seeks to put in place. As most of the part of the Act, the objective behind the establishment of the data protection authority is quite misplaced.[13]To put things in perspective, the Act actually does make no mention of the objective behind establishment of the authority and proceeds merely by explaining the nature of the institution. It is submitted that a holistic provision on the existence of the data protection authority will set forth the ground for having a more autonomous body in place. The provision for the establishment of a data protection authority in this form shall lay the foundation of an independent body that has enough resources, infrastructural and financial capability to pursue its objective in a truly autonomous manner.[14] The provisions stipulating the existence of at least 3 Joint Privacy Commissioners will ensure a greater degree of transparency and accountability within the authority. At the same time, keeping in consideration the mass unawareness towards the right to privacy, a separate coordinate of the Authority for promoting the importance of right to privacy shall be optimal to the establishment of a robust data protection regime in safeguards to the citizens against any attempts from the part of the state to infringe the right to privacy of the citizens. In what comes as the most unfortunate and disappointing aspect of the proposed data protection bill is the office of the Data Protection Authority.[15] What the bill envisages is not a data protection authority even in the remotest sense. The proposed authority is just an extension of the central government with no element of independence and accountability mechanisms in place.

The following are some of the most crucial aspects of the data protection authority that the proposed bill seeks to put in place. As most of the part of the bill, the objective behind the establishment of the data protection authority is quite misplaced. To put things in perspective, the bill actually does make no mention of the objective behind establishment of the authority and proceeds merely by explaining the nature of the institution. It is submitted that a holistic provision on the existence of the data protection authority will set forth the ground for having a more autonomous body in place.[16] The provision for the establishment of a data protection authority in this form shall lay the foundation of an independent body that has enough resources, infrastructural and financial capability to pursue its objective in a truly autonomous manner.

The provisions stipulating the existence of at least 3 Joint Privacy Commissioners will ensure a greater degree of transparency and accountability within the authority. At the same time, keeping in consideration the mass unawareness towards the right to privacy, a separate coordinate of the Authority for promoting the importance of right to privacy shall be optimal to the establishment of a robust data protection regime in the country. A separate wing of the commission for monitoring state surveillance will also go a long way in preventing the state's intrusion within the private domain of individuals.[17]

Need For A Transitional Period

India is by far one of the least privacy conscious countries in the world. The Indian awakening into

[13]Ananthapur R. India's new data protection legislation. Scripted. 2011;8:192-201.
[14]Talukdar S. Privacy and its protection in informative technological compass in India. NUJS L Rev. 2019;12:1- 11.
[15]Basu S. Policy-making, technology and privacy in India. Indian J Law Technol. 2010;6:65-70. [Duplicate entry]
[16]Joshi U. Online privacy and data protection in India: A legal perspective. NUALS L J. 2013;7:75-77.
[17]Bali V. Data privacy, data piracy: Can India provide adequate protection for electronically transferred data? Temp Int'l Comp L J. 2007;21:103-106.Roy A. Data protection: Why a comprehensive law is needed. The Financial Express. Available from: https://www.financialexpress.com/opinion/dataprotection-why-a-comprehensive-law-is-needed/1694205

an era of privacy consciousness is yet at an extremely nascent stage. The menace of misinformation and lack of awareness plague the transition of India into a privacy conscious society. The suggested Data Protection Law is all set to introduce revolutionary changes in the ways one views their data. As of now, a huge chunk of Indian population who have been at the epicentre of the digital revolution in the country have scare idea of anything known as Data protection law. It is submitted that the data protection law isn't just a regulatory mechanism, instead it's an instrument that would alter every aspect of the digital society that we line in. Thus, it is optimal to first create a sufficient degree of awareness about the right to privacy and right to informational privacy in particular to mark the beginning of a meaningful data protection regime in the country. A data protection law isn't a tonic that can be injected into the Indian society overnight to transform the prism through which the Indian view the right to privacy. It must be noted that no amount of rights conferred upon the data principals and obligations placed upon the data fiduciaries will materialize the vision of a healthy data protection regime in India. The first step has to be the creation of awareness amongst the citizens about the aspects of informational privacy both amongst the data principals and the data fiduciaries. This is the sole reason that India needs a transition sphere which would be a sort of buffer period that would ensure the transition of India from a privacy indifferent society to a data privacy society. The previous draft bill (Data protection Bill 2018) had acknowledged the need of a buffer period that would be required for the transition of the Indian society into a privacy conscious society which would understand the need for the informational privacy. It is submitted that unless there is an awareness amongst the mass about the worth of their privacy, all the substantial provisions recognizing their rights will fall into abeyance. Moreover, a complete overhaul of the Data protection regime in a country as vast as India, will prove to be a cause of the ruckus. The draft bill had incorporated the need of a transitional phase and had included a detailed framework for the date of establishment of the Data Protection Authority and the sunrise and sunset clauses to ensure a smooth transition to the new regime. However, the Personal Data Protection Bill, 2019 does not contain any reference whatsoever about the buffer period that would enable the transition.[18] It is suggested that the bill should incorporate a definite time frame under which the provisions of the Act will come into force. Failing which, the data fiduciaries too might feel a lot of confusion regarding the new provisions which would eventually give rise to serious problems in implementation. It is also suggested that a clear cutoff date for implementation of the provisions of theproposed Act shall set forth a clear architectural framework for the implementation of the provisions of the law, failing which, it might take years for the law to come into force. Thus, it is suggested that the provision based upon the transition phase be added to the proposed bill. The provision may be on the following lines; A data protection law must not only recognize the rights of the individuals, it must provide a mechanism conducive to the enforcement of such rights. The bill in present form gives undue emphasis to the interests of data fiduciaries as far as the rights of the data principals are concerned.[19]

The pendulum of convenience has been swinging in favor of the data fiduciaries from the very begging of the digital revolution and the data protection regime in India should do all that is needed to

[18]Personal Data Protection Bill, 2019. Bills of Parliament; c2019. India.
[19]Bhageshpur K. Council post: Data is the new oil and that'sagoodthing.Forbes.Availablefrom: https://www.forbes.com/sites/forbestechcouncil/2019/11/ 15/data-is-the-new-oil-and-thats-a-good-thing/#4bd8a6473045

place the rights of the data principal on the driving seat.[20] The onus to prove compliance of the provisions of the proposed Act must be placed upon the data fiduciaries and the regime should felicitate the involvement of data fiduciaries in becoming more privacy conscious and thus there is a pressing need to incentivize the common Indians to enforce their rights within the law. While, the parliament is yet to finalize the Personal Data Protection Act, 2023.

[20]Expert Committee. Report of the Financial Sector Legislative Reforms Commission. Government of India, 2013, 1.