



Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2021 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

The Exigency to address the personal data issues: The Personal Data Protection Bill, 2019

Aman Pandey^a Hema Chaudhary^b

^aLucknow University, Lucknow, India ^bLucknow University, Lucknow, India

Received 14 October 2021; Accepted 27 October 2021; Published 30 October 2021

The 21st century has witnessed the evolution of technology as never before. Countries across the globe have been permeated with this evolution & are consistently working to harness it for their economic growth to which India is no exception. Over the Years, India has also seen a major leap in technological progress but as the famous saying goes every aspect has two sides so this is the case here also. As India is transitioning to become a digitally-driven economy the major obstacle is the protection of the data privacy of its citizens. Right to the Internet is a fundamental right of citizens to which access to safe usage of the Internet is an intrinsic part. The Major Issue with the digital-driven Nation is that there is the enormous quantum of data exchange with public & private entities across unrestricted geographical territories which makes it complicated for the local authorities to securely administer & store the data of their citizens. As a citizen, once the purpose for which the data was required is fulfilled, we do not concern about where our data is going to be stored or who may have access to it. Thus, the situation is grave as the data we share may come into the hands of someone whom we never wanted to have access to. Another major setback that often citizens suffer is Internet fraud whereby they lose a significant sum of money. The citizens who are struck by this misfortune due to their undermining acquaintances are unable to find a requisite resolution to their problems. Thus, this article is basically concerned with the analysis of the upcoming data protection regime to ascertain whether the said law is dynamic to survive with the unprecedented enhancement of the digital era along with the mechanism & methods to prevent the roadblocks in the digital transition of India.

Keywords: *accountability, administer, data protection, digital, legislation, information, right.*

INTRODUCTION

As India is firmly transitioning to become a Digitally driven Nation, the question which is often being put forward is how the personal data of the citizens is being administered? The 21st Century has digitally revolutionized the globe and India is also permeated by it. Over the years citizens have inclined themselves to lead a digitally driven lifestyle. The positive consequence of such inclination is access to services at doorsteps even in times of pandemic which is only the result of unriddled technological advancement. It is pertinent to understand that the predominance of technology has reached to such an extent that we cannot even imagine our survival without it. But have we ever thought that whenever we seek or share information on the internet some way or the other, we share our personal & professional data with private & public entities? We are not much bothered about how our data is being administered once our interest is satisfied for which we had shared the data, this laxity on our part gives rise to the problems because we are unaware as to where the data is being stored & processed after the purpose has been served. This may be led to a substantial privacy breach as the data would be in hands of someone to whom we never wanted to have access to. The citizens also being uninformed about their rights in reference to personal data sharing are severely seen in dilemma once they are struck by the misfortune of any data breach or banking fraud. It is important to understand that the technology-driven market is gradually expanding and the big tech companies are looking forward to penetrating into the markets across the globe where they have not yet put their hands in. Uber, one of the largest Taxi service companies owns no cars of its own, Facebook one of the giant social media handles creates no content, Airbnb, the largest accommodation providing facility owns no hotels, these are some of the examples, there exist an innumerable number of companies who have harnessed the technology for their economic advancement with almost zero capital investment. However, the data they store and use is a matter of concern. Firstly, due to unrestricted geographical transfer of data & secondly by the absence of appropriate legislation to deal with processing & storing of the data. These situations attribute to the unregulated use of data, unauthorized leaks, hacking, data theft & thereby leaving none but the citizens to suffer the consequences.

Thus, to tackle all the issues which a technological-driven Nation could face the government is consistently working towards adopting dynamic legislation i.e., the Personal Data Protection Act, which not only could deal with the issues arising presently but to also adapt contemporaneously with the evolution of the technology. Currently, the Information Technology Act, 2000 & Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 are the prominent arsenals in the Indian legal context to deal with problems of data processing. Section 43A of the IT Act, 2000 provides for the methods of personal data protection. It is pertinent to note that it applies only to the corporate entities & therefore several government organizations that collect & process personal data do not fall within its ambit. In the present context the celebrated judgment in the case of *Justice K.S. Puttawamy (Retd.) v Union of India*¹ has substantial value wherein the right to privacy has been held as an intrinsic part of the Right to life & personal liberty & further that the right to privacy encompasses the right to have personal data protected. Thus, the judgment not only recognized the right to privacy as the fundamental right of the citizens which was inherent but dormant over the years but also evidently states that the necessity of personal data protection is undeniable.

Recently the Reserve Bank of India had put forward its idea of introducing a Central Bank Digital Currency (CBDC) & thereby is planning to have a phased implementation of it which may gradually have a major impact over the traditional physical currency. The idea is to curtail the needs of Digital payment demands however there is no presence of any appropriate legislation which may tackle the administration of data breaches which may occur during the transaction, also a plea has been filed in the Hon'ble Apex Court seeking directions to the government to frame a robust legislative policy to deal with the matters of online banking fraud² through which around 18% of the Indian citizens are victimized in the past year as reported by Business Insider. Thus, the government has to understand the ground reality of

¹ *Justice KS Puttawamy (Retd) v Union of India* (2018) 1 SCC 809

² *Hariram Morya & Anr v Reserve Bank of India & Ors* Civil Appeal No 5523/2005

the situation where a majority of citizens lack digital literacy³, the presence of a proper & effective redressal mechanism is essential before bringing in any *method which involves data risks, especially economic*.

The Upcoming Data Protection Regime, currently under scrutiny by the Joint Parliamentary Committee, has to be robust in its protections. The Bill as the Ministry of Information & Electronics cites, is based on seven key principles i.e., Technology agnostic, holistic approach, informed consent, data minimization, controller's accountability, structured enforcement & Deterrent penalties. The lawmakers have adopted an enormous approach to cover most of the possibilities that the law may face. The cross-border data flow, localization of data, application to both private & public sectors are some of the other significant features which may be seen in the Act. The regulatory approaches in the form of command & control, self-regulation, co-regulation could be seen in the regulatory authorities which will be an independent body to oversee the enforcement of data protection law.

Now just examine each of the principles to have a comprehensive knowledge of how the legislation is going to function.

1. **Technology Agnostic:** It is well established that law is not known for its stillness, it is ever-evolving & dynamic. The former Chief Justice of India, **Ranjan Gogoi J.** had also articulated that "*both art and the law witness Diversity in interpretation, the difference being that while in the former, there is a stillness, the law is dynamic, ever-evolving and progressively opening newer political arenas for the society*"⁴ therefore, the data protection law will be no exception, it will have a dynamic nature i.e., it will function & evolve with the new technological advancements thereby enabling itself to deal with new issues that may subsequently arise thereof.

³ Prashasti Awasthi, 'Over 50% of students don't have access to internet: Survey' (*The Hindu Business Line*, 17 February 2021) <<https://www.thehindubusinessline.com/news/education/over-50-of-students-dont-have-access-to-internet-survey/article33859585.ece>> accessed 10 October 2021

⁴ Mehal Jian, 'The Law Derives its Life and Temperament from the Diversity of Interpretation: CJI Ranjan Gogoi' (*livelaw.in*, 2018) <<https://www.livelaw.in/the-law-derives-its-life-and-temperament-from-the-diversity-of-interpretation-cji-ranjan-gogoi/>> accessed 10 October 2021

2. **Holistic Approach:** The data protection law seeks to adopt a holistic approach in regard to its applicability. The law would apply to both public, private sector & even to foreign entities dealing with the personal data of Individuals in India therefore, no room will be left for the public sector entities to escape their accountability which was evident in the antecedent law dealing with personal data. However, the bill will carve out different obligations for the respective entities for specific legitimate reasons.
3. **Informed Consent:** Consent is the most important part especially when we are dealing with the personal data of a citizen. However, consent itself is not essential unless it is an informed one, which the bill seeks. Informed consent means meaningful & rational opinion as to the effect it may cause to one's own interest. Thus, the person giving the consent would be entitled to know as to how his data is being processed or used & any data process which transgresses the limit for which the consent was obtained would attract accountability & liability from the concerned authority or company. The provision of withdrawal of consent has also been mentioned, where the data principal has reasons to believe that the purpose has been completed he may withdraw the consent to continue to have access to data by the fiduciary. The Karnataka High Court had restrained to sharing response data of persons collected due to lack of Informed Consent by the Centre & NIC.⁵
4. **Data Minimization:** Another significant principle upon which the legislation will subsist is data minimization. It will basically enable the public & private entities to collect minimal data as would be sufficient to serve the purpose or for other compatible purposes. All the collected data will be duly encrypted as a safeguard. Thus, this will bring relief to the citizens as they would know what data has been administered by them & the purpose behind such administering.
5. **Controller's Accountability:** Accountability is one of the features which is essential to develop transparency & faith among the citizens. The legislation seeks to hold the controller accountable for any data breach or privacy issue whether they have

⁵ *Anivar A Aarvind v Union of India* WP No 7483/2020

processed the data themselves or have transmitted it to any other organisation to process it.

6. **Structured Enforcement:** The lawmakers have kept stringent eyes on adopting a strong statutory body to redress grievances of the citizens & also to look over for the proper & structured enforcement of the data protection law. Thus, implementation has been kept into focus as the law relates to technological advancement which gradually evolves and a timely check on the working of the legislation is substantial in that respect.
7. **Deterrent Penalties:** The law is seeking to bring some stringent penal provisions which may take effect in matters of wrongful data processing. The Penal provision would be such that it will be adequate to create a deterrent effect in the society & ultimately prevent the data breach issues.

There are some other features also which the law enshrines within it other than the aforementioned basic principles, one of such provisions is in relation to the concept of Localization of Data which seems to tackle cross border data exchange issues. Once implemented, the entities will be forced to store the data within the territorial limits which if they don't comply will definitely have their businesses affected adversely & may have to face penal liability, consequently affecting big tech giants like Facebook, Google, Amazon escape from their accountability. The bill has also clearly enumerated the grounds whereby the personal data of an individual could be processed without his consent these includes, for purpose of legal proceedings, for providing benefits to the individual whose data is processed & for a medical emergency but not otherwise. Thus, other than these situations personal data of an individual cannot be processed without his consent & therefore any such data processing which falls outside the ambit of the above situations will amount to a breach of data privacy and consequently will attract penal liability.⁶

One of the other important aspects which must also be taken into consideration by the lawmakers should be the structure of the General Data Protection Regulation (GDPR) which is the prominent law on Data Protection & Privacy in the European Countries. Though it is agreed that the Laws of the European Union may not be suitable to the Indian legal system

⁶ Personal Data Protection Bill 2019

due to the peculiar circumstances however the standard and ideas which they have adopted to frame the legal backbone of the GDPR could undoubtedly be of vital significance for the Indian scenario.

Lastly, it could be rightly stated that the analysis of the key provisions of the upcoming law clearly makes it a competitive weapon to deal with digital problems. However, the lawmakers must derive the nature of the provisions in a flexible way leaving scope for wider interpretation when necessary as it is not possible to reasonably apprehend all the situations which a citizen may face. Further Digital literacy-oriented programs particularly in regard to everyday digital issues which the citizens may encounter & their redressal, must be introduced in order to acquaint the citizens with the remedies they could opt-in in case they suffer a digital complication as a law which is not beneficial to its citizens has no significance. Thus, the time is high to bring the legislation as soon as possible because as the technology evolves new facets of issues may arise which the current legislation will lack to address. Thus, all these fascinating features make this upcoming legislation a prominent arsenal to thrash away the data administering & privacy breach issues which the citizens are facing consistently so that the upcoming digitally-driven nation does not have roadblocks to evolve harmoniously.