CRITICAL ANALYSIS OF DATA PROTECTION LAWS IN INDIA

AUTHORS-

VISHWAS GUPTA, UPES

NANDINI MATHUR, MANIPAL UNIVERSITY JAIPUR

NIMISHA AGRAWAL, MANIPAL UNIVERSITY JAIPUR

Table of Contents

Critical Analysis of Data Protection Laws in India

Introduction

A populistic phrase has now taken forefront in the common parlance, i.e. 'Data is the new Oil' or 'Data is the new Crude'. If one analyses the origins of this proclamation, he/she has to take a glance in history when mineral oil or crude oil was the most prized asset and an extremely valuable commodity. Since, the Oil Bloom, many countries or rather almost every state was toiling hard to increase the reserves of crude oil in the mid-20th century. However, it is safe to presume that Data or Digital Database to be precise has swapped oil to possibly the best prized asset of the 21st century. This stance is clarified by the datum that top five financially appreciated corporations globally are Google LLC, Apple Inc., Microsoft Corporation, Amazon Inc. and Facebook Inc[1]. Interestingly all of these financial conglomerates belong to the Information Technology Sector and precisely data sector. When one compares the two products with utmost clarity, it could be easily inferred that 'Data' and 'Crude Oil' are akin to each other. Crude Oil or as it is commonly called Oil is found in its underdone form is not consumable at all and requires decontaminating and purifying for its appropriate use by conversion into commercially viable products such as Petroleum, Gasoline, Diesel, Kerosene, NAPTHA, Petroleum Jelly, et cetera. Likewise, data in its primitive form is only a raw form of facts, figures, statistics and information al needs to be administered, examined and furbished for transforming it into variegated forms of commercially consumable data. For instance, Statistics and Figures revolving around Healthcare Industry, Geological Information, Financial Facts and Figures, Online Encyclopaedias, Career-Oriented Information, et cetera.

Since the inception of World Wide Web in 1989, the importance of data was consistently recognized globally by the people and the enhancement in its importance was gradual[2]. However 2020 was the year in which the world saw the ultimate rise in essential nature of the most valuable phenomenon introduced to the world by the institution entitled as internet or World Wide Web. It is a very well-known fact that the Coronavirus pandemic was the

[1] Admin. (2019, December 4). *Top 10 company in the world | InnovativeZone magazine*. InnovativeZone. https://innovativezoneindia.com/top-10-company-in-the-world/

[2] Gillies, J. M., Gillies, J., Gillies, J. A., & Cailliau, R. (2000). *How the web was born: The story of the World Wide Web*. Oxford University Press, USA.

inhibiting factor in the sudden rise in prominence of the Data Flow and an ever increasing stock of databases.[3] Since, the globe went into a physical lockdown, no manual work could have been done. That's where the data flow came into limelight, the whole education industry, food industry and whole lot of variegated corporations shifted their workload online. The databases of different customers proved to be handy for many industries and it can be safely inferred that the only blessing in disguise by the peril invoking Covid-19 pandemic was that it exposed the unlimited monetary and humane centric benefits of Digital Data and its flow.

Before diving deep into the technical aspects related to Digital Data or commonly called as Data. One needs to understand what data is and its types. The pure form of computing data which is also referred to as Digital Data needs elucidation to become consumable information. Binary Number System is used to epitomize this form of computing data. Now this data in computerized form is then converted using soft wares to transpire into Commercial or non-commercial yet consumable information.[4] Geographical Data, Logistic Data, Cultural Data, Natural Data, Scientific Data, Meteorological Data, Statistical Data, Transportation Data and Financial Data, et cetera are some types of commercially consumable Data. This list is not exhaustive and there are a lot of other categories coming up because of technological advancements and also because of the ever growing needs of the modern world.

However, for an individual from non-IT background, Data can be generally categorized as public data and personal data. The data available, obtainable and reachable to masses in general is categorized as Public Data, such as, proceedings, records and archives of Courtrooms, birth and mortality statistics, Memorandum of Association & Articles of Association of a company and other general details, et cetera.[5] Contrary to this, personal information and details of an individual or institution/ organization which includes browsing details of an individual, pictures, personal preferences, financial and monetary records, details of one's family, physiognomies and personality traits of an individual, last location and travel particulars, behavioural aptitudes and so on are accounted as Private data. Private data is thus intimate

[3] *DATA in the time of COVID-19*. (2021, March 12). Open Data Watch. https://opendatawatch.com/what-is-being-said/data-in-the-time-of-covid-19/

[4] OECD Glossary of Statistical Terms. OECD. 2008. p. 119. ISBN 978-92-64-025561.

[5] *What is public data?* - Definition from WhatIs.com. (2013, June 20). SearchCIO. https://searchcio.techtarget.com/definition/public-data

information of an individual being or organization and cannot be dispersed by anyone without any erstwhile consent of the owner of that data. [6]

Every boon has a bane attached to it. Similarly, data breach is a bane attached to the boon entitled as Digital Data. Majority of the data breaches are concerned with private data. The number of data breaches is only increasing day by day instead of evolution of complex data protecting softwares. Data Breach can be either be committed by an individual or an institution/organization. A data breach leads to a lot of chaos and interference into the private space of a lot of people and even large corporations. A data breach can have both tangible and intangible damage, Tangible damage can be classified as financial loss while Intangible Damage can be mental harassment of the victim. It is true the intangible damages cannot be ignored but tangible damages are in a way better limelight than the intangible ones. To safeguard the global internet users from data leaks, the term, 'Data Protection' comes into place.[7]

The literal meaning of Data Protection is the procedure of preserving significant data from exploitation, conciliation or forfeiture. Moreover, these breaches also causes downtown which can cause Billions of loss in a few hours. Data Protection is a preserving method, technically trained personnel are appointed to safeguard the valuable information. However, from a legal point of view, Data Protection Laws are needed to create some sort of deterrence in the society in regards with invoking peril in the minds of potential individual who can commit data breach.[8]

For a long time India as a nation did not have a precise enough legislation which centrally focused upon Data protection and Data Privacy. India's sole controlling instrument for data privacy and its protection was the Information Technology Act, 2000 and its analogous rules, especially Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. Moreover, Personal Digital Data is also given protection under the canopy of Article 21 of the Constitution of India and has also been affirmed somewhat by the protection given by the Indian Supreme Court in various judgements where in the Apex Court avowed that information including concerning an individual and the

[6] *Stevens, Gina (10 April 2012). "Data Security Breach Notification Laws" (PDF). fas.org. Retrieved 8 June 2017.*
[7] Belangia, D. W. (2015). *Data breach preparation*. https://doi.org/10.2172/1172869
[8] De Guise, P. (2020). Contextualizing data protection. *Data Protection*, 19-26. https://doi.org/10.1201/9780367463496-2

refrain to tweak into that information without the consent and prior permission of that individual is canopied well within the domain of Right to Privacy.[9]

One of the silver linings of the overall bad year stricken by Covid-19 Pandemic was the exorbitantly increased emphasis of Databases and Data Flow. Keeping this change in mind, the Indian Government in first quarter of 2020, took a proactive and prominent step to in techno-legal policy and data regulation & guidelines, in regards with non-personal data, Digital Data related to healthcare industry, fiscal data, and information pertaining to to e-commerce and additional consumer fronting amenities and facilities. In the meanwhile, the Indian Judiciary also made a few annotations regarding personal data privacy in various judgements, and last but not the least, the ever-mulled over *Personal Data Protection Bill, 2019* ("**PDP Bill**") was a poignant move suggested by Central Government deliberation during 2020.[10]

This paper would thus primarily focus upon the evolution of the Data protection laws in respect of the Indian legal framework. The different types of data breaches and instances where in data breaches have wrecked a lot of havoc would be discussed too. A critical legal analysis of the Personal Data Protection Bill, 2019 would also be covered in the paper. The Personal Data Protection would not only be analysed constitutionally & in tandem with the Municipal Indian laws. Further, one of the research questions in this paper also covers the way forward for Indian Legislative to present a well drafted legislation in the parliament to comprehensively curb the problem of data breaches and bolster Data protection in India.

Types of Data Breaches and Major Breach Incidents in India

To understand the severity of the requirement of proper and astute Data Protection laws, it is quintessential to understand the impact of different types of data breaches on an individual and also on an organisation or an institution. Some of the most common type of Data Breaches known in the technical world are as follows:

- Stolen Information

[9] *Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors*., WRIT PETITION (CIVIL) NO 494 OF 2012.
[10] "The Personal Data Protection Bill, 2019". PRSIndia. 11 December 2019. Retrieved 21 December 2019.

This one of the most common and out rightly one of the most dangerous form of Data Breach. It may sound blatantly foolish to claim it but humans are error prone and they often commit silly mistakes. Some errors by employees can be worth crores of loss to their company. Example of one such data breach is when an employee of apple hastily left the prototype of new Iphone open in his desktop. Consequently the specifications of the unreleased device was surfacing over the internet. Information can be stolen in a number of ways within the brisk of a second. However, it is not necessarily essential that carelessness of an individual would be the only reason for stolen information. There are a lot of shrewd hackers who steal information with an evil intent to sell on the information for monetary gains.[11]

- Password/Pin Breach

  Password or Pin or for that matter CVC/CVV breach is also a common form of data breach in which severely sensitive information of an individual are at stake as a result of a cyber-attack upon his account. More precisely when CVC/CVV of an individual's monetary cards are breached, huge financial loss can easily be deliberated.[12]

- Key Strokes Recording

  Another method of data breach is key strokes recording. In this method, the cyber attacker installs a key stroke recording software in the vulnerable device and thus uses the saved information regarding key strokes to decode Personal Data. However, this type of data breach is extremely difficult until and unless there is some sort of negligence on the part of the vulnerable individual.[13]

- Phishing

  Phishing is a type of Data Breach in which the cyber attacker creates a duplicate webpage of a prominently used website and the vulnerable person mistakenly enters his credential in the forged webpage and let go off his/her sensitive information to the

[11] Moshkovich, D. (2020, April 21). *7 most common types of data breaches and how they affect your business*. HubStor. https://www.hubstor.net/blog/7-common-types-data-breaches-affect-business/

[12] *The effect of bad password habits on personal data breach.* (2020). International Journal of Emerging Trends in Engineering Research, 8(10), 6950-6960. https://doi.org/10.30534/ijeter/2020/538102020

[13] Nyang, DaeHun; Mohaisen, Aziz; Kang, Jeonil (2014-11-01). *"Keylogging-Resistant Visual Authentication Protocols"*. IEEE Transactions on Mobile Computing. 13 (11): 2566–2579.

attacker. This type of breaches is more significant in regards with financial websites and social media websites.[14]

- Ransomware

  Ransomware is a kind of malevolent and spiteful software that strains and hassles an individual or an organisation to pay some monetary amount after it has initiated a cyber-attack on their mainframe computer structure. The victim of the attack is forced to pay the ransom demanded as the software threatens to tarnish and subdue the quintessential data on their computer system if they fail to comply with the fiscal demand. However, even after the payment of ransom there is no guarantee of the restoration of data.[15]

- Malware or Virus

  Malware or virus is also known as layman's data breach as it is one of the most popular and oldest sort of data breach. Virus Attacks or malware attacks have been in prominence since the late 20th century. It is safe to claim that virus attacks are now obsolete because of strong Anti-Virus or Anti-malware software emerging up in the recent past. However, every now and then there is always a risk of a new fatal virus or malware popping up.[16]

- Distributed Denial of Service

  This type of cyber-attack is generally committed by well-coordinated cyber attackers as their target are big corporations or prominent institutions to malign their image or prove their point. More often than not this attack is stereotypically committed to signify protests. For example, if justice seeking trolls like Anonymous make their mind up that they do not like the way an exorbitant financial conglomerate like IKEA functions and feels it is taking undue advantage of their customers, then they can start a Denial of Service Attack. In this category of data breach attack, the attacking group would make it improbable for the employees of the vulnerable institution to access the computer system. It is not always essential that the data is lost, however this type of attack forces

[14] Wright, A; Aaron, S; Bates, DW (October 2016). *"The Big Phish: Cyberattacks Against U.S. Healthcare Systems"*. Journal of General Internal Medicine.
[15] Hassan, N. A. (2019). Responding to ransomware attacks. *Ransomware Revealed*, 203-212.
[16] Mohanta, A., & Saldanha, A. (2020). Malware components and distribution. *Malware Analysis and Detection Engineering*, 165-188

a corporation to freeze their work causing them financial loss. Individuals are rarely the victim of these type of attacks.[17]

- Man In The Middle Attacks

  Man In the middle Attacks are quite similar to phone tapping. In phone tapping, a third party can intervene into the conversation of two persons over a cellular device. Similarly, Data packets sent from one individual to other are retrieved illegally in Man in the Middle Attacks for unsolicited benefits.[18] Technological researchers have confirmed that data packets can be retrieved by a third party in 3G, 4G and even the up and coming 5G platform.[19]

- Data On Sale by large corporations

  There have been a lot of instances in the recent past where in gigantic IT companies have sold the information of their users and subscribers to third parties for huge monetary benefits.[20] One such instance was the Cambridge Analytica case, in which the Chief Executive Officer of Facebook, Mark Zuckerberg was brought under trial for infringing privacy of over Billion of its users.[21] These breaches are taken very severely now as it has a massive trust breaking effect on masses.

- Insider Threat

  Insider Threat is not a technical data breach instead it is a manual one where in the employees of an organization leak sensitive information of the corporation to its direct rivals or whosoever interested for monetary or some other sort of benefits.[22]

There have been a lot of instances globally where either one or other kind of data breaches mentioned above have had a massive negative impact globally. Though, there have been certain instances particularly in India where a huge amount of data was breached and used illegally attackers and culprits. It is really important to highlight those breaches to understand not only

[17] DDoS prevention. (2016). *DDoS Attacks*, 170-185. https://doi.org/10.1201/b20614-11
[18] Prowell, S., Kraus, R., & Borkin, M. (2010). Man-in-the-Middle. *Seven Deadliest Network Attacks*, 101-120.
[19] Mohamed Amine, Q., Jordane, L., & Olivier, R. (2020). Hardware man-in-the-Middle attacks on smartphones. *Forensic Science Today*, *6*(1), 012-015.
[20] Sumner, S. (2016). Supermarkets and data brokers. *You: for Sale*, 49-68.
[21] Briant, E. (2020). *Propaganda machine: The hidden story of Cambridge Analytica and the digital influence industry*. Bloomsbury Publishing.
[22] Gelles, M. G. (2016). Introduction – Insider threat today. *Insider Threat*, 1-18.

the impact of data breaches but to ponder upon the ways to curb them legally. These are some of the few notable instances where in an enormous amount of information was breached and privacy of a large number of individuals was compromised:

- Police Exam Database Breach

  It is one of the most recent data breaches with a really large impact on the Indian Bureaucratic system. In this data breach which took place in February 2021, the information of about 500000 police exams candidates furbished online for sale using a database sharing platform. Technology Security providing firm Cloud SEK traced back the information leaked online to a Police Exam conducted in December 2019. Personal information such as mobile numbers, email address and even past criminal records were leaked online.[23]

- Big Basket User Data Breach

  A cyber intelligence firm entitled as Cybel whose base is in Atlanta revealed in October 2020 that the information of Big Basket's subscribers was put for sale online. Personal information of up to 2 crore users was readily available for sale for about 20 lakh Indian rupees. The information leaked consisted of email IDs, passwords, mobile numbers, residential addresses, IP addresses, et cetera.[24]

- Data Breach of Unacademy users

  Unacademy is a start-up which is an amalgamation of technology and education. The company itself revealed in May 2020 that due to a cyber-attack on its database around the information of 2.2 crores of its users had been compromised. The information which included username, passwords and email addresses were put up for sale on dark web.[25]

- State Bank of India Data Breach

  In January of 2019 it was disclosed by an anonymous internet security researcher that the most reputed and largest bank of the nation, State Bank of India left one of its servers unfortified by dwindling to safeguard it with a password. The vulnerability to cyber-

[23] Ghosh, S. (n.d.). *The biggest data breaches in India*. CSO Online. https://www.csoonline.com/article/3541148/the-biggest-data-breaches-in-india.html

[24] *"Explained: How big is the Bigbasket data breach?"*. The Indian Express. 12 November 2020.

[25] CISOMAG (7 May 2020). *"Unacademy Suffers Data Breach; 22 Mn Users' Records for Sale"*. CISO MAG | Cyber Security Magazine.

attack was sourced to a complimentary service provided by SBI to its customers entitled as 'SBI Quick'. This service sent notifications about Account Balance and current debit/ credit dealings to its customers. Over 30 lakh messages were suspected to be compromised as a result of the breach.[26]

- 2016 Debit Card Data Breach

  Over 32 lakh Debit cards from various Indian banks were said to have been compromised in October 2016 due to malware inoculation in the Hitachi payment services system. The malware made it accessible for the hackers to extract money from accounts of compromised users who used ATM and Point of sale services provided by Hitachi. The banks who suffered most from this breach were State Bank of India, ICICI, Yes Bank, Axis Bank and HDFC. Approximately Rs. 1.3 crores of losses were reported as a consequence of fraudulent transactions by the national Payments Corporation of India. The breach went unreported for over a month and the victim banking institutions were notified and forewarned when deceitful dealings were reported by several international banks based in China and United States of America. As a result of which, State Bank of India forfeited around 6 lakh debit cards and reissued them. This was one of the largest debit card replacement drive in the Indian banking history.[27]

- Aadhar Data Breach

  Indian Government's identification database Aadhar managed by the Unique Identification Authority of India was reported to breached in early 2018.[28] Aadhar is like a social security number which possesses the information like names, date of birth, gender, bank details, Pan Card details, biometric data of over 120 crore residents of India. The data leak first came into limelight when anonymous sellers on WhatsApp, telegram and even dark web were spotted selling non-prohibited access to Aadhar database for meagre costs.[29] Moreover, an Indian news daily entitled as Tribune claimed that over 1 lakh former employees of UIDAI had access to the Aadhar database

[26] January 31, Prasad Ramesh on; 2019 (31 January 2019). *"SBI data leak in India results in information of millions of customers exposed online"*. Security Boulevard.
[27] *"Multiple banks hit: 3.2 million debit cards compromised; how it happened, what happens now?"*. The Indian Express. 21 October 2016.
[28] Whittaker, Zack. *"A new data leak hits Aadhaar, India's national ID database"*. ZDNet.
[29] Doshi, Vidhi (4 January 2018). *"A security breach in India has left a billion people at risk of identity theft"*. The Washington Post.

even after termination from their job.[30] Another leak was spotted when it was known in common parlance that state-owned LPG distributing company Indane's computing system was breached and Aadhar information of its consumers were available online for unrestricted access.[31] Moreover, Aadhar information of 13 crores Indian residents broke on the internet due error in the servers of around 200 government websites made the information public. However, UIDAI continuously denied any sort of breach on its part. Nonetheless, World Economic Forum reported Aadhar Breach to be one of the most huge data breach globally in its Global Risk Report.[32]

It is thus evident by highlighting these data breaches that Cyber Attacks have a huge economic impact on a nation's premier individuals and is an enormous blow upon the Digital privacy of its residents[33] which makes it all the more necessary for the Indian legislative to come up with a stout legislation to curb the menace of Data Breaches and robust Data Protection laws in India. Hence, in the next chapter of the paper the evolution of data protection laws in India would be discussed till date.

Evolution of Data Protection laws in India

The necessary characteristics for fortification and safeguard of personal data can be located in variegated statues in India. Some of the notable statutes that deal with the protection of personal data in India are the Information Technology Act, 2000, the Credit Information Companies (Regulation) Act, 2005 (safeguarding Financial Personal Data), the Right to Information Act, 2005 and the Aadhar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016. Apart from this statutes, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and he Information Technology (the Indian Computer Emergency Response Team and Manner

[30] Service, Tribune News. *"Rs 500, 10 minutes, and you have access to billion Aadhaar details"*. Tribuneindia News Service.
[31] *"Aadhaar: World's largest ID database exposed by India government errors"*. The Economic Times. *Retrieved 8 December 2020*.
[32] *"Aadhaar Data Breach Largest in the World, Says WEF's Global Risk Report and Avast"*. Moneylife NEWS & VIEWS. *Retrieved 8 December 2020*.
[33] National Academies of Sciences; Engineering; and Medicine, & Forum on Cyber Resilience Workshop Series. (2016). *Data breach aftermath and recovery for individuals and institutions: Proceedings of a workshop*. National Academies Press.

of Performing Functions and Duties) Rules, 2013 ("Cert-In Rules") were specially notified in public domain for increased clarity on legal framework in India regarding protection of Personal Data. Last but not the least, the constitutional framework inherently includes protection of personal data under Article 21 of the Indian Consitution and after the famous Justice Puttaswamy[34] judgement this stance has only elevated in significance.

Information Technology Act, 2000

Information Technology Act was the first and foremost legislation which recognized the importance of data flow on internet and acknowledged the protection of personal data accessible on servers of different corporations and institutions. The Information technology Act is precisely aimed to safeguard data which is specifically electronic or rather digital in nature which by the way of literal interpretation mentioned in statute refers to electronic record or information that in any stage was processed or is deliberated to be processed in an electronic manner. Apart from this, the IT Act also controls and standardizes other characteristics of internet consisting of cybercrimes and e-commerce. The patent objective of the 2000 Act is direction and expedition of data flow in the electronic commerce industry. To meet this objective, Section 43 as a provision was institutionalized in the Act to impose punitive sanction on a wide spectrum of acts and omission to do certain acts in regards with Digital data, computing systems and other computing resources. These acts include acquiring access to a computing system without prior consent of the individual owing rights over the device, duplicating and reproducing data, cyber attacking, inflicting viruses and malwares in a computing system, tarnishing and devastating data storages, damaging central processing unit of a computing system, repudiating access to the owner of a computing system, terminating or altering information contained in a database.[35]

Moreover, as per Section 43 A of the Act, a business conglomerate or a corporation not depicting due diligence towards institutionalizing and maintain appropriate safety practices and as a consequence amounting to wrongful gain or loss to any individual is liable to compensate for damages caused to that individual. For instance, in the case of *Poona Auto Ancillaries Pvt. Ltd. v. Punjab National Bank*[36], a monetary amount close to Rs 80 lakhs was debited from the

[34] *Supra* Note 9.
[35] Gupta, A. (2011). *Commentary on information technology act: With rules, regulations, orders, guidelines, and reports*.
[36] *Poona Auto Ancillaries Pvt. Ltd. v. Punjab National Bank,* Cyber Appeal/4/2013.

account of the complainant to a third party without the consent or permission of the complainant. When the matter was investigated, it was found that it was the negligence on the part of Punjab National Bank that caused a malfunction in its computing system and hence the transferee cannot be located. Thus, the adjudicating officer decided that it was the fault of Punjab National Bank and ordered the bank to compensate for the damages incurred by the complainant. Besides the civil liabilities prescribed under Section 43-A, Section 72-A of the Information Technology Act provisions for punitive sanction for revealing 'Personal Data' or "Personal information' by any Internet Service Provider, without acquiring the permission of the individual owning the data or in breach of a legal instrument with such individual with a deliberation of causing wrongful gain or loss. For any illegal activity of such nature, this provision invokes a criminal sanction of three years in prison and/or a fine of up to Rs 5 lakhs in regards with deliberate or imprudent revelation of a person's sensitive personal information obtained by a legal instrument and thus breaching that legal instrument by disclosing that information without any prior consent of the data subject.[37]

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, was formulated under authority provisioned by Section 87 (2) of the IT Act read with Section 43A of the 2000 Act. It mandates much wider defence of the personal data of individuals and as well as institutions. These rules meet up to one of the most basic necessities of data protection: permission, notification collection restrictions, usage limitation, corrective modification and onward transfer of information encapsulated in respective databases. The Privacy rules provides for the corporate entities to comply with prescribed procedures when they are included in activities consisting collecting, processing and storing personal data of different individuals.

Moreover, it compressively distinguishes between the 'Personal information' and 'Sensitive personal data or information' ("SPDI") as a sub category of personal data. In accordance to the act, personal information is defined as any information which is associated with a person and either directly or indirectly in amalgamation with alternate information which is available to a corporate conglomerate, is able of locating such individual. The Privacy Rules recognise the

[37] Sharma, V. (2011). *Information technology law and practice*. Universal Law Publishing.

following personal information as SPDI:- passwords; financial information,; medical archives and past records, biometric information; any aspect concerning to the above as delivered to body corporate for providing amenities; and any information acknowledged under the above by body corporate for dispensation, stockpiled or administered under legalised contract.[38]

Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 ("Cert-In Rules")

Cert-In Rules levy obligatory announcement and notification necessities on service suppliers, intermediaries, data and information centres and commercial bodies in the happening of definite kinds of "Cyber Security Incidents" comprising unsanctioned admittance of IT systems or data. The Cert-In Rules define "Cyber Security Incidents" as any actual or supposed contrary events, in association to cyber security, that disrupt any overtly or indirectly appropriate security dogma, resulting in: unapproved access, rejection or commotion of service; unlawful use of a computer resource for processing or stowage of information; or fluctuations to data or information without sanction.

Other Sectoral Legislations

Other sectoral legislation which aim to protect Digital data of an individual are: the Indian Contract Act, through a binding contract read with Section 43A of the IT Act, 2000. The Copyright Act by preserving the duplication and reproduction of data, The Aadhar Act, 2016 by providing for provision protecting the personal information stored under the Aadhar Database, the Credit Information Companies (Regulation) Act, 2005 safeguarding Financial Personal Data and the Consumer Protection Act, 1986 repealed by Consumer Protection Act, 2019 which protects the personal information and sensitive data of the consumers.

Analysis of Personal Data Protection Bill, 2019

Prior to the introduction of Personal Data Protection Bill in the Indian Parliament in the first quarter of 2020, three similar bills were presented in the parliament as private member bill

[38] Processing 'sensitive' personal data. (2003). *Data Protection for Library and Information Services*, 41-44.

namely, Personal Data Protection Bill, 2006, Data protection Bill, 2010 and Personal Data protection Bill 2014.[39] In 2018 too, a bill was introduced but it garnered a lot of controversy. Hence, as a result, Personal Data Protection Bill, 2019 was presented in the parliament by the ruling government to institute a legislation which is specifically drafted for the requirements of a robust Data protection legislation in the country.

Observations

These are the two observations garnered after the analysis of the bill introduced in 2019:

1. National safety is better aided by rationalising state oversight to avert information surplus and replication of exertion.

In a co-dependent and data-copious realm, government admittance to information is an indispensable but deficient requirement to ensure optimal national security outcomes. Economy whose nodal basis is information technology is predisposed by a multifaceted ecosystem of municipal legislations, marketable selections, bilateral measures, and global norms and establishments. In an ecosystem akin to the above-mentioned one admittance to data and information in a way to safeguard the society's ever-enhancing digital usage. However, this is not a way which can be incorporated in solitude and has to be amalgamated by other methods, for instance, transparency and answerability outlines for tech-based podiums, revised bilateral data-sharing legal agreements, and coordination and collaboration with international security institutes.

However, in all the instances where in acquiring access to data and information is quintessential for the government and is in national interest, the onus is upon the government to formulate access norms as literally as possible, consisting crystal clear requirements on the circumstances under which information can be brought into admittance, the exact nature of data that can be pursued and the motive for which it can be allowed admittance. Further than causes of state capability, preventing overburden of data is a cyber security imperious too.

A vast list of institutions which stockpile sensitive information also enhances the scope for malevolent state and non-state conduct. Excusing agencies of state functioning without evidently demarcated national safekeeping tenacity or without recognized fortification canons

[39] Dubey, R. K., & Verma, A. (2019). *Data protection and privacy implementation: Indian perspective.*

might well make them prone to analogous hazards. Rationalized state authorities will be increasingly favourable in making sure that they do not invade the visibly defined strictures on the shield of discrete individual civil liberties, and empower acquiescence with time-honoured jurisdictive and legislative criterions for policymaking national safekeeping action.[40]

2. **Spawning co-operative and pecuniary significance from digital data will necessitate restructuring laws and rubrics in the arenas of arcade control and rivalry, contractual law, intellectual property rights, taxation, and international trade.**

Both public and personal data will most probably be consumed in a variegated spectrum of commercial and state ventures, and will be shared, transmitted and handled transversely across numerous players. Expediting this flow of information will entail harmonizing and empowering administrations. Solemnizing possession assemblies will be critical to this exertion. Personages, industries and the government essentially share a mutual lexis on the diverse types of information and the defence principles afforded to them.

The Organisation for Economic Cooperation and Development (OECD), for instance, recognizes[41] three extensive classes of data (private, proprietary and public), and at least additional four sub-categories constructed on the derivation of data.

The Indian government will also have to generate new-fangled commands for distribution of data among manifold patrons that take into explanation contemplations of rivalry, intellectual property rights, confidentiality and cyber security. The European Union, for illustration, has acknowledged[42] four impending different prototypes for cloistered segment to government data sharing: homogenising data sharing contracts; data donor-ship models, akin to Corporate Social Responsibility (CSR) compulsions; new intercessory establishments, such as data trusts; and supervisory facsimiles for public interest causes in the turfs of healthcare, finance, transportation, etc.

It has to be restated that the Data Protection Bill ought to be perceived as one device in a predominant planning that influences data to aid growth consequences. Supervisors should be

[40] Naavi. (2020). *Personal Data Protection Act of India (PDPA 2020): Be aware, be ready and be compliant*. Notion Press.
[41] OECD (2019), "Enhancing Access to and Sharing of Data : Reconciling Risks and Benefits for Data Re-use across Societies".
[42] Staff Working Document, "Guidance on sharing Private Sector Data in the European Data Economy", European Commission, April 25, 2018.

cautious of endeavouring to accomplish through the Bill aftermaths that could be healthier attained using other policy treadles.

Recommendations

Section 35: Power of the Central Government to exempt any agency of government from the application of the Act

Section 35 of the 2019 Bill authorizes the Central Government to subject coherent orders relieving any government organisation from the necessary provisions of the Bill for aims and motives enumerated in the provisions of the Bill.[43]

Comprehensive exceptions and deficiency of exclusive or jurisdictive precautions will flop in meeting the guidelines laid down by the Supreme Court in the K.S. Puttaswamy v. Union of India[44] case, where it stated that methods confining the right to privacy must be supported by law, assist a genuine aim, be parallel to the objective of the law, and have procedural protections against exploitation. Imprecise grounds that activate exclusions, absenteeism of procedure in yielding exceptions, and the dearth of autonomous omission are some major concerns in regards with this provision

The 2019 Bill is a stride in regressive direction in contrast to the Personal Data Protection Bill, 2018 as it ominously enlarges the latitude of immunities while instantaneously weakening significant protections. While national safeties may in some cases supersede individual importance in privacy, it is precarious, as the Justice Srikrishna Committee stated[45], "to ensure that the pillars of the data protection framework are not shaken by a vague and nebulous national security exception".

The following considerations shall be taken into notice in regards with Section 35 of the Personal Data Protection Bill, 2019:

[43] Draft of the Personal Data Protection Bill, 2019, as introduced in Lok Sabha, Parliament of India by Ministry of Electronics and Information Technology, Bill No. 373 of 2019.
[44] K.S. Puttaswamy v. Union of India, 2017 (10) SCC 1.
[45] Committee of Experts under Chairmanship of Justice B.N Srikrishna, "A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians", Submitted to Ministry of Electronics and Information Technology, 2018.

1. Grounds for exemptions

Terminologies like 'sovereignty', 'integrity', 'state security', 'international relations', and 'public order' are accountable to be construed instinctively and require unblemished strictures that would generate exceptions. Private Members' Bills in regards with Data Protection which presented in parliament in earlier instances and other government reports on personal data fortification may provide direction in judicially tweaking the provision. For instance, The Private Member's Bill presented by Shri Baijayant Panda in 2017[46], enlists five explicit grounds in accordance to which the state may confine the right to privacy. Likewise, the Intelligence Services (Powers and Regulation) Bill,[47] presented by Shri Manish Tiwari in 2011, providing for eight descriptions to determine circumstances in which national safety was under hazard.

2. Scope of exemptions

Compulsions like just and rational dispensation and execution of defences must endure smearing even to discharged government involvements. Furthermore, it would be incongruous to strip the Data Protection Authority of its supremacies to avert the misapplication of personal data or to stipulate codes of virtuous data protection practices. Indemnities in the national interest should, therefore, not outspread to the wholeness of the PDP Bill and must be restricted to definite lots, as was the case in the PDP Bill, 2018.

3. Principles of lawfulness, necessity, and proportionality

The "necessary and expedient" typical in the present Bill skirmishes with engrained legal ideologies for secretarial action and the Supreme Court's decision in the *Puttaswamy* judgement. Exclusions should be settled under the buff of law as disparate to executive orders. Moreover, the PDP Bill shall postulate that excused processing must be essential and impartial vis-a-vis the purposes of the law. Section 42 of the PDP Bill, 2018, is an upright socket of orientation as it already comprises of legal provisions that give consequence to these principles.

[46] Draft of the Data (Privacy and Protection Bill), 2017, Bill no 100 of 2017 as introduced in Lok Sabha, Parliament of India by Shri Baijayant Panda, Member of Parliament.
[47] Draft of the Intelligence Services (Powers and Regulations) Bill, 2011, Bill No, 23 of 2011 as introduced in Lok Sabha, Parliament of India by Shri Manish Tewari, Member of Parliament.

Section 91: Government Access to Anonymised and Non-personal Data

Section 91 of the PDP Bill empowers the Central Government to direct data fiduciaries and data processors to allow admittance to all anonymised or public data. This provision is established on the postulation that unencumbered entree to definite groupings of data is crucial for the besieged conveyance of government services as well as supplementary state purposes such as "growth, security, integrity and prevention of misuse".[48]

Non-personal data is probable to aid a broad spectrum of public utilities. However, familiarising such a sectoral provision in the current Bill is precipitate, given that the Ministry of Electronics and Information Technology has instituted a professional commission to inaugurate an outline for the authority of non-personal data.

The paper highlights the following concerns for the JPC to consider:

1. Grounds for government access to non-personal and/or anonymised data

There is a prerequisite need for purer explanations or law-making criterions for state functions that certify access to non-personal and anonymised data. Most commercial companies involve in accumulation of sundry data sets, which encompass both personal and public data, and afford these data sets distinctive shield contingent on whether the information was poised based on human input, arithmetical corollaries, or additional means. Lack of shared nomenclature between government, commercial institutes and society in general could dent the affluence of doing trade, thwart data sharing exertions and destabilise privacy rights.

2. Definitions and standards for anonymised data

Anonymised data demarcated under Section 3(2) of the Bill is data that has endured an "irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified". Irretrievable anonymization is improbable— an avowal that is

[48] Draft of the Personal Data Protection Bill, 2019, as introduced in Lok Sabha, Parliament of India by Ministry of Electronics and Information Technology, Bill No. 373 of 2019.

buoyed by the Justice Srikrishna Committee Report along with other government[49] and educational[50] study. Data Protection Authority must primarily recommend canons for anonymization and consequences for fissure—preferably variegated criterions based on the type of data and amount of jeopardy—before facilitating the state to entree public data.

3. Ethical considerations

An apprehension looms that Public or anonymised data and information might comprehend prejudiced inputs or interpretations. Positioning these data cliques for public purposes jeopardies aggravating prevailing social, political and economic disproportions. It is suggested that data that has been attained or certified for public utilities must endure a social influence or ethics review afore being arrayed towards gratifying public policy goals.[51]

Conclusion

Given the existing dynamic and continuously intensifying scenario of Information Technology sector in India, which is abounding with challenges, aggregating overseas investments and monetary progress in an ever-expanding digital epoch, there is an extraordinary necessity to apprise privacy, confidentiality and data protection laws and criterions in contour with international ingenuities which are seasoned and already in practice. The absence of all-inclusive and dedicated legislation, while a substance of distress, has been counterbalanced by topical inventiveness by the industry, the public and the government. These ingenuities pursue to fetch in the desirable lawful charter while accompanying the prevailing guidelines and the pre-emptive sentiments and to stand by the judiciary to guarantee evading bodies are held answerable for not effectively shielding personal data. It be hooves corporations looking for institute business in India to observe to the municipal laws particularly in the milieu of the

[49] "Opinion of Anonymisation Techniques" adopted by Data Protection Working Committee, European Commission,10 April, 2014.
[50] Rocher, L., Hendrickx, J.M. & de Montjoye, Y. "Estimating the Success of Re-identifications in Incomplete Datasets using Generative Models". *Nat Commun* 10, 3069, 23 July, 2019.
[51] Arora, H. (2019). Grounds for lawful processing of personal data in GDPR and personal data protection Bill 2018, India (PDPB): Section – VI: Legitimate interests. *SSRN Electronic Journal*.

cumulative thoughtfulness of the Indian legal framework towards data protection and privacy apprehensions.

While the 2019 Bill has tranquilized some of the rigorous and inflexible provisions instituted under the Personal Data Protection Bill 2018, it also appears to insipid some of the striking characteristics of the legislation that purposes to guard the privacy rights of individuals. Keeping in mind the mounting necessity of the digital economy, having a supervisory framework in tandem may be the quintessential requirement, however, providing the government with unfettered and comprehensive supremacies to immune government agencies from the legal obligations of the 2019 Bill for certain conditions may overthrow the tenacity of the 2019 Bill and endanger a person's fundamental right to privacy. The 2019 Bill is still to be reviewed by the Joint Parliamentary Committee and the shortfalls will hopefully be addressed before the same is finalized and brought into effect. The 2019 Bill is expected to have a far-reaching impact on Indian businesses and multinational corporations doing business in India.

2020 has positioned the footing and foundation for a conduit of progresses and advances on the data privacy and data fortification obverse. While one may easily observe the oblivious latitude and essentiality of the Personal Data Protection Bill, still it is necessary that the bill is improved and enhanced in the spectrum of proposes before it is reintroduced in the Parliament in coming days. An observer of IT sector in India could also assume noteworthy guideline on the pecuniary and moneymaking usage of non-personal data, as well as possession characteristics. The Personal Data Protection Bill 2019 may also be made obtainable and accessible for dialogue and stakeholder annotations, clarifications and interpretations once the swotted variety is unconfined. The situation on data localization and cross border sharing of data is yet to be confirmed and concluded, which is a policy pronouncement that will impact and affect most of the businesses functioning in India. However, in the backdrop of the Personal Data Protection Bill, an individual can anticipate to endure observing industry-specific data policies, guidelines, criterions and regulation by sectoral regulators and authorities such as drone-related policies and guidelines which might give escalation to new issues, problems and disputes including cybersecurity and obligatory revelation to the Government of India. It is also unblemished that the judiciary is more conscious and acquainted of privacy rights than ever before, which is an insignia of a strong data protection and fortification regulation ahead.