EQ. CITATION: BNWJ-0720-015

4. The Personal Data Protection Bill, 2019

By: Aishwarya Kumar

Pg. No: 45-58

EQ. CITATION: BNWJ-0720-015

i. Abstract

Recently in Houston, the Prime Minister of India quotes, 'Data is the new oil, new gold' which made it clear that India has entered the next level of dependency on the internet Industry 4.0 is completely based on data. For the cheap availability of data in India, it requires laws that make it not only cheap but also secure. As India looks forward to a free and fair digital economy, we must make sure it must be safe and secure. As the COVID-19 takes over the country the internet has become our solutions for everything. From businesses, government rules, educational institutes, and even concerts are online. This means the amount of data available is humongous and without proper regulation, the data is vulnerable to all sorts of abuse. Data fiduciaries and Data principals as discussed in the bill must be responsible and accountable to each other with regards to the storage and control over the data. India finds its way to the bill which is inspired by the existing laws in other common law countries. This paper deals with in-depth meaning, usage, and issues in the cyber world. It also explains the cyber laws in the world and why data protection is of prime concern. The Indian perspective is also discussed which pulls out a few flaws.

EQ. CITATION: BNWJ-0720-015

Table of Contents

S. No.	Title	Pg. No.
i.	Abstract	46
1.	Introduction	48
2.	Data Thefts and Cyber Crimes: The Dark Web	49
3.	World Legal Set-up	52
4.	The Personal Data Protection Bill, 2019	55
5.	Conclusion	57

EQ. CITATION: BNWJ-0720-015

1. Introduction

Data protection is to safeguard and protect data from being corrupted and misused. It is extremely important to protect this data as data is created every second and stored when it is shared in different cloud storage. Data protection also helps to quickly restore data after its corruption or loss. The right technique of data management is necessary to protect data. Data management is of two types: data life cycle management which deals with systematic and strategic movements of data from online to offline storage, information life cycle management which deals with the protection of data from applications, malware, viruses, and even user errors. Data availability is a different concept altogether which ensures that irrespective of malfunction of data in the system, it must be available so that there is business continuity. This happens by replication or duplication of data whereas data management archiving data in a way that the corruption does not take place of is minimalized. The only thing common is the option of backing up data that helps to do both management and availability of it. This concept is the 'backup' which means to replicate or mirror data files and store them separately so that if the original is affected in any way, they may be restored by the means of these replicas created and stored.

Data portability is a facility that provides for the movement of data from one application to another similar to cloud services. Cloud services are used by people and businesses to store data online on public or private clouds to back up their data. This proves as a solution to data management and data availability but poses a problem for data protection. Backups have been an effective solution for the problem of corruption or system failure. The mirroring of data is done and stored in clouds online and will stay there until the primary data storage is distorted and these duplicate files substitute them. The issue that comes up here is that if these cloud services fail or get hacked there is a huge chance of misuse of these files. There will occur breach of private data, business secrets, private strategies, or any other damage to the owner of these files. Hence, data protection is extremely essential, and legal aid for such disputes must also be available as internet breach of rights is similar to breach in person.

Continuous Data Protection (CDP) is a process of creating a single copy of the backup array instead of replicating multiple copies and saves any modification made to the original copy so

that when the need arises it serves the same purpose[63]. This is revised and a better version of the backup system, as it serves as a backup with modification similar to the original but the chances of misuse remain. The technological aspect is taken care of by bringing in the revised version to reduce the risk factor but what also needs to consider that with an increase of internet usage and web dependence all our personal and business data is prone to being corrupt and laws and remedies against such breach of rights is extremely important.

2. Data Thefts and Cyber Crimes: The Dark Web

Data theft or Data breach is unauthorized access into data and personal files of the system which may be misused against the owner leading to damage of reputation and business which may take a lot of time to repair. As our dependence on the internet increases, cyber attackers also do an increase in a similar ratio. Corporate firms, business organizations, famous identities are attractive targets to these criminals. Data theft often leads to either any monetary damage or compromise on identities and selling this personal data on the dark web that is extremely dangerous. Few reasons that may increase the scope of data theft could be out-dated software, weak passwords, spamming and phishing attacks, downloads from unknown or non-verified sites which may lead to the download of the malware. In the year 2018, an organization called 'Dubsmash' was booked under breach of data and selling data identities of over 162 million user accounts. They sold it to companies such as MyFitnessPal and a dating site named CoffeemeetsBagel[64]. The company had no explanation on how the database access was provided to these firms. The greatest data theft scandal reported was the 'Facebook- Cambridge Analytica scandal' which shook the entire reputation that Facebook had earned as it has more than a billion-user base spread across the world, and has managed its privacy so-called efficiently. The scandal brought-forth the importance of privacy of the individuals who are trusting the network with their data. Facebook sold a vast number of user data for political

[63] Rouse, M. (2019, August 21). What is Data Protection and Why is it Important? Definition from WhatIs.com. Retrieved July 11, 2020, from https://searchdatabackup.techtarget.com/definition/data-protection.
[64] Swinhoe, D. (2020, April 17). The 15 biggest data breaches of the 21st century. Retrieved July 11, 2020, from https://www.csoonline.com/article/2130877

needs[65]. Another incident was by Yahoo who claimed that there occurred a data breach of almost 500 million accounts and also claimed it to be a state-sponsored one. These incidents of data breach clearly show the fact that data is not safe as hackers get through the database and steal data or the company gives access to their database at some cost. One way to improve the status of this is to consider the quality of data. If you are entering your name and age then a certain amount of protection is provided and if you are submitting your credit card number or even your phone number, this data will have more protection so that it is not easily accessible[66].

Data thefts are a subset of cybercrimes that pose a threat to all sorts of identities that exists on the world wide web. Cybercrimes are increasing as criminals utilize the web to steal, gain and misuse data. This may include the use of personal data, business data, government data, or even disable the device in use. Crimes may be related to target networks or devices or maybe gain access to confidential and unauthorized information for personal interests. These crimes could be targeted to property which could be stealing bank credentials and misusing them by making purchases or simply stealing money, or targeted to an individual by cyber stalking and encouraging virtual prostitution, or targeted to the government database and hacking into the confidential information of the state and drafting strategies to cause damage to the state. These attacks may be in the form of installing malware in documents that may be downloaded by the user in the future by Potentially Unwanted Programs (PUPs) or Phishing mails. Attacks on networks are generally executed by way of DDOS attacks by trafficking the network so that the website is overwhelmed with the response that it stops functioning and the network goes down.

The Cybercriminal Justice System has also been established to combat these crimes and regulate this sector as misuse of the internet information will shake every industry, every organization. To plan and execute a cybercrime it takes 200 days. Few ways you can prevent yourself from being a victim from such crimes is by updating your passwords, vigilant while browsing websites, use antivirus protection, and do not click on any unknown emails or links sent. Preventive measures will be the most effective ways to avoid cybercrimes but the

[65] Lapowsky, I. (n.d.). How Cambridge Analytica Sparked the Great Privacy Awakening. Retrieved July 11, 2020, from https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening.
[66] Data Theft Definition | Cybercrime.org.za | Safety & Security Guide. (n.d.-a). Retrieved July 10, 2020, from http://cybercrime.org.za/data-theft.

remedies provided by the justice system established is determined to protect the rights of the users and keep a check on any illegal activity reported and take required measures to combat it. Cyber health must be promoted and awareness must spread as every corner of this country, from the richest of the rich to the poor smartphones, has made its way. After the launch of Jio's strategies and policies, everybody has access to the internet. Hence cyber health must be discussed and debated upon to increase understanding of the virtual world we are living in.

Terrorism attacks have evolved with time, and have spread not only geographically but also changed their interfaces to cyber-attacks. Cyberwarfare and cyber terrorism are two grievous attacks aiming at the government and the state itself making it highly dangerous. Cyber terrorism came into light when WannaCry was exposed in the year 2017 which led to cyberattacks all over the world that targeted Microsoft office systems by inserting ransomware crypto worm and demanding money by way of cryptocurrency[67]. To prevent this Microsoft came up with the 'kill switch' that made sure the prevention of the spread. The attack affected about 2,00,000 computers across 150 countries. Cyber threats are becoming more advanced these days and with businesses shifting from register records to databases it increases the risk and with highly skilled hackers and up-gradation of technology the shift is smooth and quick. Today antivirus installed would be enough for data protection but tomorrow the same antivirus may seem worthless due to the technology change and different approaches to gain unauthorized access. The shift is so swift that now cyber-attack insurances have also started that provide for the damages caused to the business due to any cyber attacks on the computer systems[68]. It causes a lot of damage to the tangible and intangible assets of any company and the cyber insurance policies make sure to cover such damages for a given time period. Some companies provide for cyber solutions and guide businesses to manage their data in a way that they prevent from being victims of such attacks.

[67] Fruhlinger, J. (2018, August 30). What is WannaCry ransomware, how does it infect, and who was responsible? Retrieved July 10, 2020, from CSO Online website: https://www.csoonline.com/article/3227906.
[68] Wyman, O. (2017). Global Cyber Terrorism Incidents on the Rise. Retrieved July 10, 2020, from Mmc.com website: https://www.mmc.com/insights/publications/2018/nov/global-cyber-terrorism-incidents-on-the-rise.html.

3. World Legal Set-up

Amidst such attacks and vulnerability of data, the world has come up with legal measures to regulate and monitor this interface. A new sector of 'Cyber laws' came into play where regulations were passed to make demarcations of offenses online. Many countries such as the UK, Canada, and Australia have their own cyber or IT laws governing their states. Indian has the Information Technology Act,2000 which governs the offenses against property, government, and individuals. With e-commerce coming up as the safest way to do business keeping the COVID-19 condition in mind, the dependence on the internet has only been increasing. This situation has led to companies to shift to the new model of work from home by way of online platforms. Schools and colleges have resorted to online classes on platforms available. Applications like Zoom, Webex, Skype, Google meet, Google Hangouts, etc. have received a lot of online downloads. Such applications or virtual platforms are utilized to transfer confidential business information, personal data, and even government-related information. Laws need to regulate and IT laws are not quite enough to combat these problems. IT or Cyber laws are primarily for the offenses committed on social media or other e-platforms, but these data storage and its protection often go unnoticed. Offenses online are generally related to misuse or breach of privacy by a wrongdoer against the victim. Data protection is more to do with the platforms that contain our information by storing the details that we share on their website, irrespective of purpose. Data protection laws are to be established in harmony with the IT laws in that country. This situation is similar to that of consumer laws and civil laws, remedies are available in both but consumer laws focus on a certain producer- buyer relationship and their rights and duties. It is equally necessary to make sure efficient regulation of the business sector. Similarly, data protection is essential taking into consideration the rate of data theft and access of people on databases and information on the world wide web.

The United Kingdom on May 25, 2018, declared General Data Protection Rules (GDPR) all across Europe to harmonize and bring everyone to the same page in regards to data privacy and rights of individuals on e-platforms[69]. These are guidelines for organizations and e-commerce companies to handle the information they receive from users to protect them from abuse of it.

[69] What is GDPR? Everything you need to know, from requirements to fines. (n.d.). Retrieved July 11, 2020, from IT PRO website: https://www.itpro.co.uk/general-data-protection-regulation-gdpr.

It is considered to be the strongest set of data rules that exists. The core of these regulations lies 'personal data' that could be anything that directly or indirectly recognizes a living person[70]. They also have specific categories for different sorts of information databases and higher protection is assumed for sensitive information that organizations are to maintain else huge fines will be imposed. UK also has established seven principles which consider the following aspects[71]:

1) **Lawfulness:** To obtain data from the user with full knowledge and for lawful purposes.
2) **Purpose Limitation:** The purpose of the collection must be informed and consented to.
3) **Data Minimization:** Collect the data that is needed and not anything more.
4) **Accuracy:** The data must be accurate and up-to-date.
5) **Storage Limitations:** To store data until it is necessary.
6) **Integrity:** The data stored must be contained with the utmost protection.
7) **Accountability:** The GDPR must be followed and any person collecting such data is accountable for its use.

Canada on the other hand had its data protection laws in place since the 2000s itself by the Personal Information Protection and Electronic Documents Act (PIPEDA) that governs the collection and disclosure of data by any commercial organization irrespective of whether it is government-owned or private owned[72]. These were essentially based on 10 principles of care of personal data that was established in 1996 that not only inspired the Canadian laws but also the European principles mentioned above. Here the prime limitation is commercial activities or commercial organizations. Commerce related transactions will fall under this ambit of data protection even if it is a Non-for-profit organization or political parties. 'Personal Data' here stands for any piece of information that is objective or subjectively signifying a person

[70] International Comparative Legal Guides. (n.d.). Retrieved July 10, 2020, from International Comparative Legal Guides International Business Reports website: https://iclg.com/practice-areas/data-protection-laws-and-regulations.
[71] Guide to Data Protection. (2020, March 23). Retrieved July 10, 2020, from ico.org.uk website: https://ico.org.uk/for-organisations/guide-to-data-protection.
[72] Andrada Coos. (n.d.). Data Protection in Canada: All You Need to Know about PIPEDA. Retrieved July 10, 2020, from Endpoint Protector Blog website: https://www.endpointprotector.com/blog/data-protection-in-canada.

identifiable that means it is not only about name, age, ID, etc but also about comments, opinions, views, etc. Privacy Act is codified to further make sure that personal data is protected and no breach of privacy occurs. Data protection and privacy are similar but handle different aspects of the same objective and that is the prevention of unauthorized access.

Australia has legislation on federal and state levels. Federal level is the Privacy Act, 1988 that handles the way the business entities and the government have the power to store what kind of personal data. 13 Australian Privacy Principles (APP) is mentioned under this act that establishes its origin and purpose[73]. The state-level legislation may differ but must be in complete harmony with the Federal laws of the country. The three basic obligations that any entity handling data include health records legislation, federal legislation, and email and marketing legislation. These legislations with the Privacy Act make sure complete protection of personal data and no loopholes through which firms can escape. The definition under the Australian law for 'personal data' is any information or opinion that may be true or not or whether it is recorded in a material form or not, if it is enough to reasonably identify the person then it is considered personal data. The definition is quite broad and extends to most of the data as it is present on the web. One distinct feature is that the APP does not include a small business operator that is also subject to exceptions (limitations in relations to its turnover), the political party that is registered under Australian laws, a state or territory authority.

These are few countries that have pioneered in the field of Cyber and Data Protection laws and have carved the way for a better and healthier cyberspace. India inspired by these common law countries came up with the Data Protection Bill, 2019 on December 11 after two years of serious debate this bill was recommended to be presented in the joint parliamentary committee after which is likely to be passed in 2020.

[73] Law in Australia - DLA Piper Global Data Protection Laws of the World. (2014). Retrieved from Dlapiperdataprotection.com website: https://www.dlapiperdataprotection.com/index.html?t=law&c=AU.

4. Personal Data Protection Bill, 2019

The landmark case of K.S. Puttaswamy vs. Union of India[74] that laid down the 'right to privacy' as a fundamental right. Privacy is described as an inviolable space that everyone needs to be left alone. Every individual indeed needs to be conditioned by the relationships he has with the society, but this may sometimes pose as interference into personal space by raising questions against the individual's habits or character. Such issues that come up where a line is to be drawn by the judiciary concerning the reach entities can have information about a person. These are to deal with by keeping constitutional values and liberty in mind and also bring in a pragmatic solution that will favor the basic structure established. The aspect of privacy brings in Data protection as an essential aspect that is to be worked upon to improve the security level in the cyberspace.

The bill has three prime points that it launches which is privacy as a fundamental right, the increase in the digital economy as communications as faster and easier online, necessity to have a free and fair digital economy with due respect to user's privacy[75]. The jurisdiction of this bill is to all personal data processed or shared within India, any citizen or person registered under the Union, or has any connection to the business carried out in India. It may not have jurisdiction over anonymous data. The definition of 'Personal data' is inspired by the United Kingdom as it is defined under Section 3(28) to be any data directly or indirectly identifiable by any attribute of a living person online or offline for profiling. The catch in this definition is 'living person' which means any person who 's dead and any entity holding secret information about him will not come under this definition. This is a little dangerous as a dead person also leaves behind a reputation of himself, it may be disturbing to receive personal information that may not be material but enough to damage the reputation. Breaking of confidentiality of the personal data is termed as a personal data breach. This may not happen is consent to publish such information is present as defined under Section 11 of the said bill. Three main elements are to be considered while processing and collection data under this bill which is : (a) it must

[74] (2017) 10 SCC 1.
[75] GROUNDS FOR PROCESSING OF PERSONAL DATA WITHOUT CONSENT 12. Grounds for processing of personal data without consent in certain cases PERSONAL DATA AND SENSITIVE PERSONAL DATA OF CHILDREN 16. Processing of personal data and sensitive personal data of children. CHAPTER V RIGHTS OF DATA PRINCIPAL AS INTRODUCED IN LOK SABHA CLAUSES. (n.d.). Retrieved from http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

be consented as per Section 11, (b) it must be done fairly and reasonably, (c) it must collect on a necessity basis. These regulations get its roots from the seven principles of Data protection laid down as per the European laws.

Data principals or users are granted rights of getting a conformation, correcting any incorrect data, deletion of data if required, and also access to the data generated from such collection. A right that also has been granted is the 'right to be forgotten' that is similar to the GDPR. It describes the option to stop the access to the data disclosure given to the data fiduciary and the erasure of the existing data.

Data fiduciary is any entity that processes or collects data and determines its purpose as under Section 3(13) of the bill. Some exceptions are laid down for the sharing of data without consent. These circumstances are as follows:

- Any function of the State or provided by law.
- Medical treatment under epidemic or other necessary emergency circumstances.
- Safety of an individual during the breakdown of public order.
- Employment-related purposes such as recruiting, termination, etc.
- Other Reasonable reasons as defined under Section 14.

These exceptions are very similar to the exceptions in the GDPR but they are framed loosely giving space to loopholes. This is dangerous as it gives criminals reasons to get away from the offenses they commit. Obligations of the Data fiduciary are also carved out such as privacy policies as per Section 22 and transparency of the use and handling of data is to be maintained. Data fiduciaries and Data processors must have security measures that will make sure to restore the integrity and prevent misuse of data. The liability of the stored data is on the data fiduciary and his responsibility of making sure that no unauthorized access takes place.

Sensitive information is transferred outside the State then the original data must be stored in the territory and there must be explicit consent of the individual. He must be made aware of how the data will be used and the purpose of it. The exemptions from this Act can be given by the Central Government in the interest of sovereignty of the state and to avoid incitement to commit an offense. Other exemptions include investigation, journalistic, domestic, and for research purposes.

The penalty that the data fiduciary is liable to pay for non-compliance of the obligations laid down is a fine to an extent of 5 crores or 2% of the worldwide turnover whichever is higher, and the violations of the regulations will call for a fine of 15 crores or 4%of the annual turnover, whichever is higher. The misuse of identification of a person without consent that is not under the broad exception of Sections 12 to 15 will invite imprisonment up to three years or fine or both.

This bill is very similar to the GDPR guidelines established by the UK government and also the 10 principles of protection of data laid down by Canada's PIPEDA. The bill also draws inspiration from the Australian Privacy Act in the section of its exceptions of State or Federal authority and small businesses.

5. Conclusion

As the world has come online and we can assume the fact that in this generation there are two societies, one is the real world and one is the virtual world. In such a situation our data must be protected and must be secure. Any unauthorized access must be reported and such necessary legal measures must be taken. As aware users, we must make sure we are responsible with what websites we visit, what content we view, what data we disclose and what we promote online. If we are cautious and ensure safe and right us of cyberspace, it will prevent us from being victims of cybercrimes and data theft.

These rules are already applied to a few e-commerce businesses as in the form of confidentiality and privacy requirements. If this bill comes to force it will be new to some firms. This bill entails essential rules that will help to keep check of data transfers and also make people aware of their rights and duties as Data principals. This bill must be passed as soon as possible keeping in mind the dependency on the internet. There was an old draft of this bill that was not passed. The few differences or rather the improvements that have been made to suit the needs of the society are the exception to government agencies, the treatment of non-personal data, criminalization of certain actions.

Some points differ from the sources of this bill. It allows the transfer of non-personal data by other entities to the government that they have collected, to improve the government services

but fails to explain how it will happen. The usage, purpose, and objective of this data remains unknown. It also brings in this point of keeping sensitive information within the territory and requires explicit consent from the individual to transfer such data. This may bring in glitches in international transactions. This will lead to less international transactions which may affect the e-commerce a lot. In a world where e-businesses are the future, this might be a huge barrier. In cases of exemptions for the government given by the GDPR, Privacy act of Australia, PIPEDA other cyber laws caught such grey areas and regulate them, but in India with the IT Act,2000, and the exceptions in this bill, the escape will be easy. The escape in the virtual world is much faster and easier and laws must be tight and clear. India must consider its position of legislation that exists and frame laws. Although this bill touches all the aspects, it is vaguely framed. For a sovereign nation like India which likes to maintain its constitutional values and make sure equality and liberty exist, it will be complicated to frame the apt laws but it is surely not impossible.