

Data Protection in India in reference to Personal Data Protection Bill 2019 and IT Act 2000

Dr. Anusuya Yadav¹, Gaurav Yadav²

¹Assistant Professor, Law Department, MDU Rohtak, Haryana, India

²UG Student, IIIT Sonapat, Haryana, India

ABSTRACT: The ever-growing internet usage has also increased user data. This user data collectively known as Big Data is the reason behind the increasing data breaches. The data of thousands of users is compromised every day. But this is not the only threat that we are facing. Digital Advertisements are one of the greatest means of capital generation in the present time. Companies earn by showing advertisements to the users, based on their search queries. Due to this illegal use of personal and private data to increase business profits is also increasing nowadays. This is a breach of privacy concerns. In a country like India having no data protection law makes it much easier for such tech giants. Although there are a few laws regarding privacy, but all of them aren't sufficient in this internet-driven world. Now, whatever laws are there that prevent them from doing so, till now Indian citizens are dependent on them only. The proposed regimes under the Personal Data Protection Bill 2019 are expected to be much more robust in protecting data in comparison to existing regimes, which are incapable of protecting data sufficiently. This paper provides a comparison of existing and proposed rules and regulations for data protection. It also provides an overview of how personal data is used to generate capital.

Keywords: Data, Information, Laws, Rules, Breach, Theft.

1. INTRODUCTION

Increasing innovation in technologies is taking us to a new era. As we step into that new era, there come the challenges and the aids. As of now, the internet is the biggest network that connects us all, irrespective of our locations. Information sharing has been made very easy, since the existence of the internet. But, with the intensification of Cyberspace, the frequency of Cybercrimes has also amplified. Fraudulent transactions, Leakage of confidential information, Defamation, and Ransomware are the modern-day problems of digitization. Compromising data servers and authentication circumvention has become very easy with the growth of the hacker community. Various protective measures are taken by several governments and companies to protect data from attackers. Besides the upcoming technologies like IoT, Machine Learning, and Artificial Intelligence, the protection of data is still a big concern, and it's becoming a bigger threat to the future [1].

Due to the rapid increase in Internet users, the data is also increasing. This is the only reason for Data Breaches or Data Theft. Data Theft is not the only big concern, what if the data collectors try to use user data? The simple answer to that is Data Protection Laws prevent data collectors to do so. In a worst-case scenario when there are not sufficient Laws or in the absence of Data Protection Laws, it becomes a very tedious job to prevent the data collectors from doing so. Likewise in India with unfortunately no legislation over privacy and data protection, it is very difficult to prevent unintended use of user data by-product or service companies.

Whenever we use any product or service whether it is free or paid then we have to provide some information that is required for registration like the first name, last name, date of birth, email, mobile number, etc. It depends on that service or product how much information it needs from us. For example, when we install WhatsApp on a smartphone and register on it then it asks permission to access storage, contacts, microphone, cameras, etc. but if we talk about any simple application like an audio recorder then to use it microphone access has to be given. Apart from this, whatever processes happen, they run in the background. An ordinary user is not cognizant of these. So, we give our information to the company that owns the product or service to use the product or service, but we do not know anything about how that company uses our data or information that we have provided. Nowadays many companies are generating capital using user's data. This capital generation is happening based on digital advertising because the user can be tempted to buy a product or service by showing digital advertisements. For example, when a user searches for some product or service using a search engine, then the search engine stores all the records of the things searched by the user. When the results

of the search query are sent back to the user, they contain some ads related to the service or the product [2]. The following figures show how ads are displayed with the search results, and how this whole mechanism work.

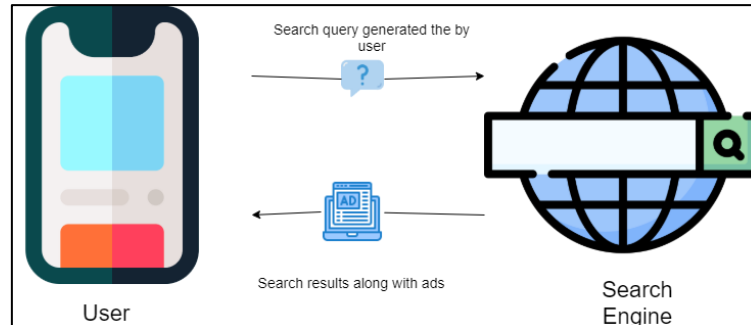


Figure 1: Ads Mechanism

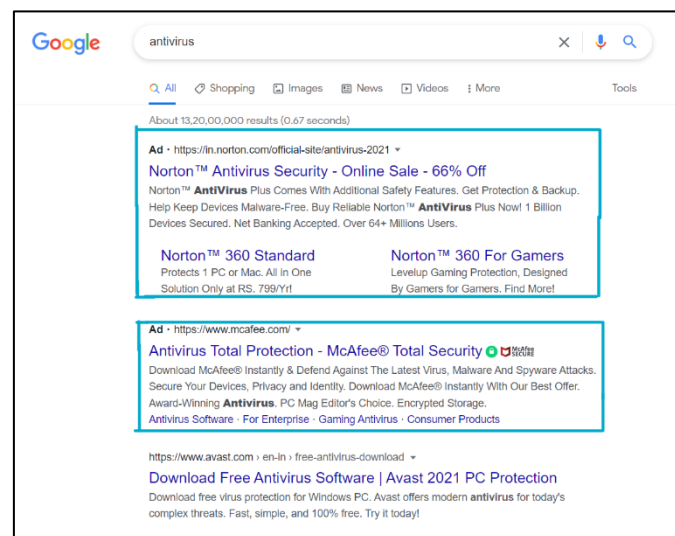


Figure 2: Ads in search results of a Search Query (Source: <https://www.google.com/search?nfpr=1&q=antivirus&spell=1>)

These promotional ads displayed to the users on behalf of product/service owners are paid, which Search engine marketing platforms like Google Ads, Bing Ads, etc. charge. Likewise, Ads can be on YouTube, Some applications, Websites, etc. Users only have two options, either usage of service/product with ads or buying a premium for the service/product [3]. So, in this way the data collectors can use the data of the users if there are no regulations.

In India, for data protection, the rules come from different sources. IT Act 2000, CPA Act 2019, rules made and imposed by different government organizations such as Reserve Bank of India, Securities, and Exchange Board of India, Telecom Regulatory Authority of India, Insurance Regulatory and Development Authority of India, etc. all these are the same sources from where talk of data protection is done [4].

Unlike India, the EU in January 2012 set out plans for even data protection and privacy. The European Union introduced GDPR, a new framework for data protection and regulation in the European Territory. Four years later in April 2016, it was approved by the European parliament, and then the newly formed legislation came into force on May 25, 2018. GDPR is applied to every organization operating within the European territory or any organization outside the European territory providing products and services to the customers of the European territories. The introduction of GDPR improved data management and the understanding of data collection [5].

2. DATA VS INFORMATION

Data and information are the same things, this is a huge misconception that usually confuses people. Data are facts that can be recorded for example text, audio, video, etc. [6]. While information is the processed data, that means information contains a meaning, but the raw unprocessed data or simply the data itself has no meaning. Figure 3 displays the relationship between data and information.

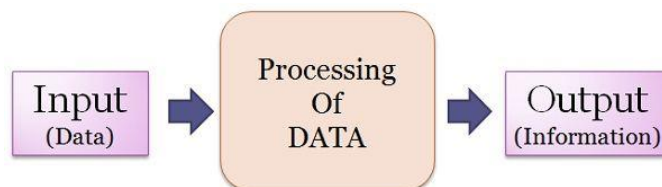


Figure 3: Processing of Data

(Source: <https://techdifferences.com/difference-between-data-and-information.html>)

But when we store the data inside the database, we use rows and columns to store it in a well-organized manner. When the data is stored neatly and cleanly so its meaning is very clearly visible [7]. Hence data breach leads to heavy damage. Figure 4 shows how rows and columns are used to store data, and how this well-organized form makes this data meaningful.

```

dvdrental=# select title, release_year, length, replacement_cost from film
dvdrental=# where length > 120 and replacement_cost > 29.50
dvdrental=# order by title desc;
  
```

title	release_year	length	replacement_cost
West Lion	2006	159	29.99
Virgin Daisy	2006	179	29.99
Uncut Suicides	2006	172	29.99
Tracy Cider	2006	142	29.99
Song Hedwig	2006	165	29.99
Slacker Liaisons	2006	179	29.99
Sassy Packer	2006	154	29.99
River Outlaw	2006	149	29.99
Right Cranes	2006	153	29.99
Quest Mussolini	2006	177	29.99
Poseidon Forever	2006	159	29.99
Loathing Legally	2006	140	29.99
Lawless Vision	2006	181	29.99
Jingle Sagebrush	2006	124	29.99
Jericho Mulan	2006	171	29.99
Japanese Run	2006	135	29.99
Gilmore Boiled	2006	163	29.99
Floats Garden	2006	145	29.99
Fantasia Park	2006	131	29.99
Extraordinary Conquerer	2006	122	29.99
Everyone Craft	2006	163	29.99
Dirty Ace	2006	147	29.99
Clyde Theory	2006	139	29.99
Clockwork Paradise	2006	143	29.99
Ballroom Mockingbird	2006	173	29.99

(25 rows)

Figure 4: View of data in Database (Source:

https://en.wikipedia.org/wiki/File:DVD_Rental_Query.png)

2.1 Public Data

Public data means all the data that is publicly exposed and does not have any national or international restrictions on its usage, modification, and redistribution [8]. For example, PDF or text on government websites, content intended for public usage, etc. Generally, open data and public data are considered the same but there is a lot of difference. Most often public data is poorly organized but the open data is well maintained and organized. And hence open data is a subset of public data, figure 5 shows that how open data and public data are related.

2.2 Personal Data

The concept of personal data was shed more light due to GDPR. Personal data refers to everything that can be used for an individual's identification [9]. For example, name, location, email address, IP address, etc. Personal data can also be in encrypted form. Any data related to an anonymous person is not considered as personal data.

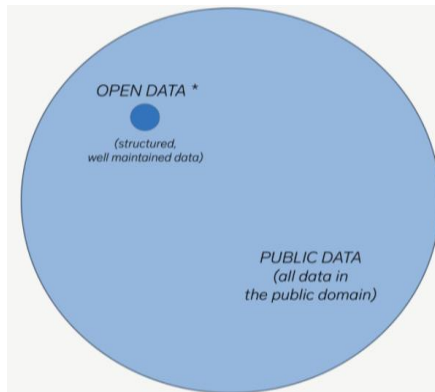


Figure 5: Public Data and Open Data (Source: <https://enigma.com/blog/post/what-is-public-data>)

2.3 Private Data

The data whose public exposure can lead to adequate damage to individuals or an organization is known as Private Data. Private information is necessarily considered to be held private. Usually, data theft or data breaches lead to private data exposure into the public domain [10]. Examples of private data are bank account details, medical records, passwords, etc. Security of private data provides quality to life, that's why data security is a big concern.

3. IT ACT 2000

Data Security Rules in India come from various sources, but IT ACT 2000 is the vastest source. It was designed and implemented considering United Nations Commission on International Trade Law, 1966 as a role model. Presently IT Act 2000, contains a majority of rules and regulations relating to Cyber Security in India. It contains several offences and punishments related to various cyber-crimes, such as IPR violations, hacking, data breaches, etc. But the presence of those many laws is still insufficient in this vulnerable security architecture. It has few provisions that try to confront crimes involving the usage of personal data. Only sections 43A, 69, 72, and 72A of this act have relevancy with data protection [11].

Under section 43A of IT ACT 2000, if any individual gains or losses due to any insecure practice of the data collector or data handler. Then that data collector and data handler shall be held responsible, and they shall be fined and that person shall get compensation. But there is no upper limit for the compensation [12].

Section 69 was amended into the IT ACT 2000 in 2008. This section states that if there is some website or application that in any manner threatens or harms India's image or relations, or something else then it can be put down or banned. Crimes and punishments in case of breach of confidentiality fall under section 72 of the IT ACT 2000. Imprisonment of two years, fine of one lakh rupees, or both are the punishment under this act. While section 72A deals with the disclosure of data, it states that if a service provider discloses the user data without the consent of the user, then the service provider shall be held responsible. Imprisonment of three years, fine up to five lakh rupees or both are the punishment under this act [13].

With several sections, IT ACT 2000 is a much vast act, but it is not very robust in the present time. The absence of laws on Domain Names, silence about taxation on online transactions etc. are some of its shortcomings. It contains several loopholes and doesn't have enough capability to tackle the present and upcoming cyber threats and crimes [14].

4. PERSONAL DATA PROTECTION BILL 2019

The Personal Data Protection Bill 2019 was drafted by the committee of Justice BN Srikrishna. There is a huge role of GDPR in its formation, mostly it is referenced from GDPR. Although this bill has not yet been passed by Parliament, this bill appears to be very beneficial according to the previous Data Protection Rules and Regulations. The Personal Data Protection Bill 2019, deals with the storage, collection, processing of data, and related penalties, compensation, and the code of conduct. The Personal Data Protection Bill classifies three types of data, general data, sensitive data, and critical data. The things covered under sensitive personal data are examples of passwords, medical records, gender status [15]. In this bill, there is a mention of the Right to be Forgotten, which means that if any company or organization uses or discloses for the financial benefit the data of any user without consent, then the user can call that company or organization may prevent it from doing so. Although everyone does not know whether our data is safe or not, anyone who tills now

felt that their data is being used in a wrong way did not have any concrete law till now for taking any strict legal action against that organization or company. But this thing has been made easy in the Personal Data Protection Bill. Now the Data Collector will have to follow all the rules which have been given under this bill. The most important thing about this bill is that the processing and storage of the critical personal data will be done only on India based servers or data centres so that our data will not go directly out of the country and this is a big deal. Under this, the user's data will not be processed or shared without consent [16]. All the rules in this will apply not only to private organizations but also to all organizations in the government sector as well. Under this bill, the government has been given the power that if it wants, it can take the non-personal data of a user from any organization. For social media also, a verification process has been mentioned in this bill so that fake accounts may reduce significantly. If a company shares any user's data without consent, then it will have to pay a fine of 15 crores or 4 per cent of global turnover or in case of a data breach, the company will have to pay 5 crores or 2 per cent of global turnover as a fine. Although it is just a bill right now India's vulnerable security structure needs an act like this very much. And the timely updation of the rules is a must.

CONCLUSION

Data security is a very important thing in this cutting-edge era. Thousands of people connect to new services every day and in the same way, the data of all the people whether it is personal or public or private increases, the responsibility of protecting it lies on the companies providing those services. And it is also the duty of these companies that they should not to use the data of the users for any wrong purpose. In the last few years, there have been many such cases in which the user's data has been used by the company for profit in business or either disclosed by mistake. Data protection laws or legislation helps a common user in securely data storage and proper usage. But in the absence of such laws, business tycoons do anything for commercial benefits. That is why it is necessary to have a data protection law. There is currently no such satisfactory law in India that prevents misuse and insecurity of user data. Last year, a game named PUBG was banned in India due to data-related issues, but now when the company changed the game and relaunched it, even now also the data of Indian users were sent to the servers located in China. If there had been such a solid rule, then the matter would have been different but it is not right now. IT Act 2000 alone cannot cover everything. Personal Data Protection Bill 2019 is a very good proposed legislation which may seem bad today but it will improve upcoming time.

REFERENCES

1. Yadav, D. A. (2020). 2.Network security and its role in controlling Cyber-Crimes. Journal of Oriental Research, XCI, 72–79.
2. Google Ads: What Are Google Ads & How Do They Work? | WordStream. (2012). <https://www.wordstream.com/google-ads>
3. Yesbeck, J. (2019, May 23). What Is SEM? A Guide to Paid Search Engine Marketing. Alexa Blog. <https://blog.alexa.com/what-is-sem/>
4. India - Data Protection Overview. (2021, June 16). DataGuidance. <https://www.dataguidance.com/notes/india-data-protection-overview#:~:text=Under%20the%20Bill%2C%20the%20DPA's,and%20promote%20data%20protection%20awareness.>
5. Lakshman, S. (2018, March 31). What is the E.U. law on data protection all about? The Hindu. <https://www.thehindu.com/news/international/what-is-the-eu-law-on-data-protection-all-about/article23401965.ece>
6. Vaughan, J. (2019, July 31). data. SearchDataManagement. <https://searchdatamanagement.techtarget.com/definition/data>
7. GeeksforGeeks. (2020, September 1). SQL | Views. <https://www.geeksforgeeks.org/sql-views/>
8. Enigma: What is Public Data? (2021). Enigma. <https://enigma.com/blog/post/what-is-public-data>
9. What is personal data? (2021). ICO. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/>
10. Private Data Definition. (2021). Law Insider. <https://www.lawinsider.com/dictionary/private-data>
11. legal Service India. (2021). Data Protection Law In India. <http://www.legalserviceindia.com/article/l37-Data-Protection-Law-in-India.html#:~:text=The%20purpose%20of%20this%20bill,damages%20due%20to%20disclosure%20of>
12. V.K. (2021). Data Protection Under Information Technology Act. Legalserviceindia. http://www.legalserviceindia.com/legal/article-4405-data-protection-under-information-technology-act.html?fb_comment_id=3790050857728200_3797189353681017
13. V.K. (2021). Data Protection Under Information Technology Act. Legalserviceindia. http://www.legalserviceindia.com/legal/article-4405-data-protection-under-information-technology-act.html?fb_comment_id=3790050857728200_3797189353681017
14. legal Service India. (2021b). Domain Name, Cybersquatting and Domain Name Dispute Resolution. <http://www.legalserviceindia.com/articles/cddisp.htm>
15. Iyer, R. (2020, January 7). The Personal Data Protection Bill, 2019. Privacy - India. <https://www.mondaq.com/india/data-protection/880766/the-personal-data-protection-bill-2019>
16. A. (2019, December 6). Union government clears the Personal Data Protection Bill 2019. Diligentias. <https://diligentias.com/union-government-clears-the-personal-data-protection-bill-2019/>
17. Madhamsetty Charitha; Nagaraj G Cholli. "Big Data Analysis and Management in Healthcare". International Research Journal on Advanced Science Hub, 3, Special Issue 7S, 2021, 42-53.
18. Dharshika S; Nagaraj G Cholli. "Green Cloud Computing: Redefining the future of Cloud Computing". International Research Journal on Advanced Science Hub, 3, Special Issue 7S, 2021, 12-19.
19. Priyanka N.; Swetha D.; Anjali G.. "Internet of Things (IOT)-Data Security Challenges and Solutions". International Research Journal on Advanced Science Hub, 3, Special Issue 6S, 2021, 144-147.