VOLUME 24, MAY 2021 ISSN 2456-9704

DATA PRIVACY AND CAMBRIDGE ANALYTICA: A CASE STUDY

By Dr Amita Verma, Associate Professor, University Institute of Legal Studies, Panjab University

By Dr Karan Jawanda, Assistant Professor, University Institute of Legal Studies, Panjab University

By Arshdeep Kaur, LL.M., University Institute of Legal Studies, Panjab University

ABSTRACT

Data privacy is an important aspect of today's digital world. With the Facebook case that involved the company Cambridge Analytica, the other side of online platforms is exposed which were behind the veil of ignorance earlier. With the rising cases of data misuse on digital space, common people are well aware of their privacy rights.

The whole responded to data misuse case of Cambridge Analytica in its own ways. In India, the need was felt for the data protection laws which are still in its initial stage and yet to see the light of days. Aftermath of Facebook case in India led to formation of various committees giving recommendations for the Data Protection Bill in compliance with GDPR (General Data Protection Rules) for European Union.

Keywords: Data Privacy, Data Protection, GDPR, Cambridge Analytica

METHODOLOGY

In this paper, focus has been made on the use of non doctrinal methodology, also known as empirical approach or a socio-legal research. This is more pragmatic and based on present day experiments which become imperative for our study. This methodology has been adopted because it focuses primarily as the observation and experiments and in our research work, the present day scenario has been observed giving special emphasis to the data protection guidelines prevalent after the Cambridge Analytica case and GDPR guidelines. The statistics and report gathered by following the non-doctrinal approach help us in carving out a true picture of what is happening in the real world.

INTRODUCTION

The data privacy concerns have widened especially after the Cambridge Analytica case and people have become aware about their personal data. There was uproar by the media as well as activists and a strong bill was recommended. Since information is the only thing that is considered to be the most important thing, especially on a digital platform, it becomes way more important to grant protection to it by some means or the other.

To protect data and sensitive information available on the digital platform it is pertinent to have a specific legislation with this regard and by following the same, the personal data of thousands of people can be saved from various threats that are prevalent. There are multiple attacks that can be experienced these days and the digital information is vulnerable as compared to other documentations. The sensitive information is at a great risk and to protect the same it is all the way important to have such an enactment that favors and protects the information available online. Owing to the digitalization, the need for having a legislation becomes essential and although there have been many enactments like the Information technology Act and

rules, the implication still seems to be inappropriate and inconsistent with the legal provisions mentioned.

The statistics and the report analysis depict that the problem of digital privacy is ongoing and will be prevalent for a longer period because of the excessive use of digital platforms and transfer of the data and personal information online. To prevent the cyber crimes that are on the high rise, it is pertinent to have a synchronized legislation for the same.

CONCEPTUAL FRAMEWORK

The term Information Privacy, synonymously known as Data Privacy or Data protection is generally a correlation between the assemblage and dissemination of data, technology and the issues like privacy of the same. It is basically protecting your data from any sort of corrupt practices or misuse of the personal information. Data privacy is generally concerned with the procurement of data, the ways it should be handled, the means and methods of saving it from threats of severe kind.

Data privacy defined the ones who are in charge of the data and the real owners or the ones to whom the access is provided. Data protection on the other hand provides certain tools and accessories so that the data is saved from the threats of the outside world. Both data privacy and protection are important to keep your data safe because data privacy will give the right to only the restricted owners while data protection will govern the rules and policies and make sure that restriction is adhered.

BRIEF ANALYSIS OF THE CASE: CAMBRIDGE ANALYTICA

A very famous incident that invited attention of almost all the people on this planet is a recent scandal that has made every head turn. This was the case which immersed Facebook Inc. and another company named Cambridge Analytica in hot water because of a whistleblower that made quite a lot of revelations. This scandal is basically concerned with the data that was obtained by millions of users of Facebook without getting their consent by a British firm Cambridge Analytica.

This firm known as the British Cambridge Analytica is a UK based data analytics firm which is usually concerned with the political agendas and campaigns. It basically takes up all the data from masses for the profiling and identification of the voters. The firm uses many types of processes for procuring the data including data mining, data collection by brokerage, data analysis, etc. It has been involved in many political campaigning and the recent one was with the elections of Donald Trump. In the year 2013, an app was made by a data scientist in the University of Cambridge named ‘this is your digital life’. By the help of this app, the firm Cambridge Analytica asked for the details of million users of Facebook and not only them but to reach masses the friends on Facebook were also invited and in this way a lot of personal information was collected by saying that the same will be used only for academic purposes. There was data from millions of users around the world. The first time it came into limelight was when a journalist reported that this firm has been using the personal information of many users with regard to the presidential election and the data that has been collected without the consent from the users.

There were many articles and journals written over these years from 2013-2017. The main information was received in the year 2018 when an ex employee of the firm confirmed the same that there has been a breach of data. As much as 100 billion dollars were lost from the capitalization of Facebook and people started approaching Facebook CEO Mark Zuckerberg for the same. He had to confront the public as well as all the politicians and testify the same. The reason why it came out so big was because the CA took out information from more than 50 million Facebook users and that information included all the personal information of the people ranging from where they live, what pages they have visited, etc. This information was later on used in political campaigns and it was nothing but the exploitation of the people and their personal information was used for their own purpose. The app or how it came out as a quiz was created by a scientist and a professor in the University, Aleksandr Kogan who shared all the information to the parent company SCL (Strategic Communication Laboratories) which later on created Cambridge Analytica.

The data that was collected was illegal in a way that it was against the data protection laws. It is because of this law that data protection laws and privacy came into force and were accepted and appreciated by masses. In the year 2014, both CA and the data scientist entered into a contract which included the use of personal information and data of the users. The data scientist used the personal information and data of million users of Facebook and supplied the same to this company CA.

AFTERMATH OF THE INCIDENT

There was a lot of hue and cry by the people who were affected by the scandal since their data was breached owing to the scam by Facebook and Cambridge Analytica Company's collaboration.

- RESPONSE BY FACEBOOK- The CEO of Facebook apologized at first regarding the whole incident and said that it was a mistake on his part and the breach was done by the company's app and it was a way to get the personal information of the people but that was an accident and it was not against their consent. An app was formed which acted as a quiz and there was a question answer format to which people responded and it did not exactly mean the breach of their data because they had consented for the same. There was no misuse of their data at first and it should not be termed as an illegal incident. The CEO apologized in almost all the newspapers and journals and also made a reassurance that there will be a strict adherence to the rules made by the GDPR and they must be followed by every single employee. The Cambridge Analytica was unfollowed by a lot of companies and they declined their support from the company. Some of the officers of Facebook called it a data breach while some were arguing that it was a mere accident and nothing was taken against the employees rather they had consented for every detail of their information.

- THE DELETE FACEBOOK MOVEMENT- After the scandal, the public reacted to this by a lot of aggression and protest by delving into the delete Facebook movement. Masses across the globe initiated the campaign and they all were in favor of boycotting the use of Facebook. Even the co owners and co founders of other such social media apps

supported this movement and participated in the same.

- DOCUMENTARY- After this incident which gained a lot of limelight and reaching to masses, there was a documentary that was released on a media platform Netflix. The name of the documentary was The Great Hack and it featured everything relating to the scam. It also provides the information related to the company Cambridge Analytica and Facebook, their backgrounds, their relationship, the app that was made, etc. It also depicts the experience of all the people involved during this case along with their respective roles. The main focus is to give a true and clear picture of what exactly was the scam and how many people were involved in the same. Also, it describes the role of each and every individual indulged in this right from the beginning, be it Mark Zuckerberg or former employee of Cambridge Analytica Brittany Kaiser who revealed their exact intention for holding the data.

- SUSPENSION OF VARIOUS APPS BY FACEBOOK- After the scandal, Facebook removed and suspended a lot of apps due to the investigation of the software developer system that was created after the case. It also banned a number of apps which were not using the data correctly. Those suspended apps were related to almost 400 developers who suffered a lot after this major scam. If any developer has failed to follow the rules and guidelines of strict regulations under GDPR, Facebook has even sued them.

- OTHER SOCIAL NETWORKS CHANGED POLICIES- After Facebook made certain changes in its privacy policies, the social networking also experienced different variants in terms of the security policies, the personal information, etc. The Facebook app also locked custom audiences so that no information is transmitted to the third party. The social media platforms now allow the users lot functions including the features like delete and edit their data. These changes have been brought because of the GDPR strict guidelines and rules.

- REVOKING OF THIRD PARTY COOKIE ACCESS- It has been announced recently by Google Inc that it will block third party cookie access in Chrome entirely and by taking this step a lot of market investors will be affected as currently as many as 70 percent of the population is using desktop services and 40 percent is using the mobile app. Therefore it can be observed that after this scandal and the post Cambridge Analytica era, there has been a great change in the mindset of the people as well as various market giants who are running on the basis of the data that is shared by millions of users. Before this, there was a gap between the data that has been shared and how and in what way it will be used and the end result of the same. Now, the things have changed and it is evident that the GDPR rules are now followed religiously by the giants as well as the digital companies in order to provide a safe environment and a secure zone where they can freely share and use their information without being monitored. However, this cannot be a truth in entirety and there are still many loopholes and hidden agreements that we have been ignoring but still the digital platform has still become a safe place.

Data is an essential commodity and an extremely important asset of a company especially who are minting money out of the data that belongs to thousands of people. Due to this incident the conversations relating to

data privacy were triggered and at least there is some awareness relating to the most quintessential part of our lives, i.e. our personal information. As a result of the scandal, a lot of things have changed and the best part about the post scandal era is that people have become aware now and they want to keep a track on their data unlike the earlier times where they were not aware about the same.

INDIAN SCENARIO ON DATA PROTECTION LAWS

The concerns of privacy can be heard loud and clear after various incidents and especially after the Cambridge Analytica scandal. Not only the firms but the people have also become aware of their data, its privacy and related factors. The Indian Courts have now agreed that Right to privacy is a fundamental right indubitably and that it must be considered as one of the Fundamental rights as enshrined under Part III of the Constitution. These new legislations and laws are spreading throughout and covering all the dimensions where there is a need for protecting the sensitive information and data. These laws emphasize on putting a control on the big giants and the companies which are exclusively dealing with such information which is highly confidential and sensitive in nature. However, such laws are somehow inconsistent with the growing menace over the digital world and efforts must be made so as to protect the most quintessential asset, i.e. the data and important information online.

The Government of India has been efficient enough and various law commission reports have been submitted and checked upon by the Justices and it has been held that a new direction has emerged out of the security and privacy regulations and an expert commission led by Justice A.P Shah is focusing on providing more recommendations and suggestions which are helpful in saving the data from the fraudsters of digital world.

The data protection law in India is currently not very clear and transparent and there are many lacunae in the whole process and system. This is majorly because of lack of any framework by the legislature. The ongoing data threats online and the cyber crimes that are on the surge have become a common problem. This is happening across the countries and there is no protection from the malpractices of the same. Since it is the digital world and technology plays its part, there are no boundaries or restrictions on the overseas transaction and people can transact and move over places online and therefore the threat of cyber crimes becomes even more dangerous. The practice of data breaches and stolen data cannot be just ignored and there is a need for some stringent rules and laws that would punish the people involved in this and give justice to the victims.

The cyber crimes are on a high rise because of lack of legislation and there is no express entry and legislation which deals specifically with the data protection laws. The Data Protection Bill was laid down in the Parliament in the year 2006 but it has never seen the light of the day.

The Government of India has created and implemented the concept of Digital India and with almost 450 million internet users, India is on the verge of becoming a digital economy and having said that the country is in the process of becoming digitally sound and for that the data transactions and the use

of data and digital information is pertinent and the protection of the same becomes all the way essential. The world of the Internet has given birth to a lot of companies including Facebook, Uber, Zomato, Air BnB, etc and these involve the transmission of a lot of personal details which must be protected and preserved from theft and such other crimes online. Since data is a valuable item, there are some concerns which make the data unsafe on the digital platform, especially their personal data and owing to this the Supreme Court has made privacy an important and fundamental right under the Constitution of India.

There are certain key regulations which are dealing with the online data related rules and these are mentioned below:

a) Information Technology Act, 2000.
b) Information Technology (Reasonable Practices and sensitive personal information and procedure) Rules, 2011.
c) Certain Rules and Regulations relating to:
    - Tele-communication
    - Banking
    - Insurance
    - Medical Healthcare
d) The Right to Information Act, 2005
e) GDPR (General data Protection Rules)

INDIAN JURISPRUDENCE

Judiciary has played a vital role always in dealing with changes and required amendments. The evolution of data protection can be traced back to the times when the right to privacy was held as a fundamental right of citizens.

- First and foremost is Article 21 which guarantees freedom and liberty to all the individuals and it focuses on the fact that no individual will be under any hardship that will hamper his/her freedom. There are however, certain restrictions but they relate to the ones which are permissible to the same extent.

- The first time the need of rights to protection and privacy was felt was in the case of MP Sharma v/s Satish Chandra (1954 SCR 1077) In this case, matters relating to the search & seizure of a person were questioned and it was held that the search of a person must be done keeping in mind the rules and procedure as well strict adherence to decency.

- Earlier, the Supreme Court did not acknowledge the said right and no recognition was given to it. It was held that Article 21 does not encompass in it the right to privacy and the procedure laid down under various other acts shall follow. The right and such protection cannot fall under article 21 of the Indian Constitution. In the case of Kharak Singh v/s State of Uttar Pradesh and others(1964 SCR (1) 332)the court held that Article 20 does not accommodate any protection and privacy right under it.

Later on in the landmark case of A.K Gopalan v/s Union of India (1950, AIR 27)Justice Subba Rao observed that personal freedom and security are an important part of a person's life. If there are several hindrances, then physical and personal freedom will not be achieved. Both mental and physical restriction will affect the freedom of an individual.

A similar view was observed by the learned Judge, J. Frankfurter in the case of Wolf v/s Colorado (338(U.S) 25 1949)that there must be no use of arbitrary power which causes

search and seizure of a person concerned. In another case of People's Union for Civil Liberties(PUCL) v/s UOI (18th december 1996) The Supreme Court observed that there is no harm in making the provision of protection and privacy inclusive of Article 21 of Indian Constitution. The rights under this Article will not be affected if any other sphere of right is inserted in it.

The issue of privacy was raised for a long time and the issue became a matter of concern in no time. It was in the case of K.S Puttaswamy v/s Union of India (CWP (1014) of 2017, 26th sept, 2018) also known as Adhar Card Case where the Right to privacy was observed as a fundamental right. The collection of personal data was held as against the right provided under Article 21, Article, Article 19, Article 25 etc. The parliament then declared this right to be a fundamental and not a basic right.

OBSERVATIONS BY JUSTICE D.Y CHANDRACHUD

- Since freedom and privacy are an inseparable part of human's lives, the right to privacy is unavoidable and right there must be a balance between the rights and requirements of the individuals.
- Right to privacy must be a given space in Part 111 of Indian Constitution and it should not be considered just a basic right.
- The meaning and scope of security is quite vast and inclusive of many dimensions including family life, sexual orientation, material status, etc.
- There must not be any law or a provision which infringe the fundamental right as enshrined under Part III of the Constitution of India. If such a provision prevails, then it would defeat the purpose of law.
- Security can be understood in two perspectives, namely -negative and positive. The negative sense prevents the state from unnecessary intruding into the freedom and personal space of an individual while the positive sense ensures that privacy is maintained at all costs.
- With the advent of technology, we are in a phase where everything and everyone is connected digitally and the focal point should be the protection and preservation of online data so that cyber attacks can be minimized.
- For a safe platform, the state must provide stringent norms and procedures that abstain from making the data vulnerable.

The scope of article 21 has increased especially after Puttaswamy Judgement but has also been reiterated in the case of R.C. Cooper v/s Union of India where along with privacy, fair treatment was also focused. After the IT Act, GDPR guidelines come as a breakthrough and the rules regulations are followed by the countries falling under the European Union. However, there are certain similar as well as differences of GDPR as compared to the Indian Laws and the following points are enumerated in this regards:

SIMILARITIES OF GDPR WITH INDIAN LAWS

1. There is a bar on collecting the personal data of an individual and minimized information is collected in the first step.
2. The provision of daily data audits and reviews is both provided under Indian provisions as well as under GDPR norms.
3. The right of consumers to transfer their preferred data is also a feature present in both.

4. The information of data protection authority and their respective supervision is also an important aspect covered under both.
5. They also provide financial penalties in case of any breach of the rules.

POINTS OF DIFFERENCE BETWEEN GDPR AND INDIAN LAWS

There are certain similarities between GDPR and Indian legislation. The India laws provide for both criminal and civil remedies in case of any breach of data or any non-compliance with the provisions, which GDPR includes a violation of fines of 20 million errors.

1. The data protection bill majority points to the collection and transmission of information within India or any countries operating and dealing with India but GDPR has its branches all over the world and in all those countries which are part of European Union.

   Thus, it becomes pertinent to draw a comparison between the Indian laws as well as the data protection bill along with GDPR rules and guidelines and it can also be observed that the law related to privacy as well as data protection is somewhat similar everywhere and it is important to safeguard the digitally acquired data. Although the branches from which the power and regulations flow is somewhat similar but the manner in which they are implemented is different and even contains some flaws. It has been viewed that there is no proper implementation of the rules of the Personal Data Protection Bill. The Indian laws have been made consistent with the present scenario and present status of the digitalization by keeping in mind the variable nature of the concept of data privacy. There have been many enactments which deal specifically with the data available online and the ways to protect the data along with other rules which come into picture after some sort of breach or crime has been committed.

CURRENT STATUS OF DATA PROTECTION BILL IN INDIA

After the Cambridge Analytica case there has been uproar among the people of India as the users have to choose between the Government and the companies that provide them with the social networking sites. They have to make a choice between the private companies and the Government policies that relate to the data protection bill. The users are worried that the only thing that they require is the control and autonomy over their data which is despite the fact that there are numerous guidelines and policies not given to them in entirety. The control over their data includes knowing all the whereabouts of their data and how and in what way their data is being accessed and processed. The users are bound to know the status of their data as to whether the data is being stored properly or not and if in any way it is being misused by the companies or not. To find out all such details the users must have access to their data and by giving them full control companies can assure them that their data is not at all misused.

KEY POINTS IN CURRENT STATUS OF THE BILL

- The Data Protection Bill of the year 2019 is supposed to be presented in the month of March 2021 and on the verge of becoming an Act if it passes the whole criteria and gets the consent.
- The main goal and purpose of the Bill is to grant the users access to their data so that the storage, process and whole system is controlled by the users.

- There are however clauses and provisions which are vague and ambiguous and those are open to interpretation by the judiciary and that can lead to misuse and overreach of the Government.

There is however no act at present in India yet but there are changes in the United Kingdom's Act and with the growth of GDPR regulations the same have been extended in India too and the privacy laws are followed in the country.

CONCLUSION AND RECOMMENDATIONS

Privacy is an essential element of our lives and the same cannot be ignored. It has always been an important part but after the landmark case, it has been given legal recognition at a greater platform. It is undoubtedly inherent valuable human rights available for every individual. Since our society is of a dynamic nature, the concept of privacy keeps changing and this varied right might as well involve various other phrases of privacy itself.

The right to privacy has been recognized as a fundamental right which has also been into limelight after the famous Puttaswamy case. Although India has very strong historical incidents that support privacy law still to gain such momentum in the modern world, this case delivered justice to it. In the international perspective, privacy has been the talk of the town since the adoption of the Universal Declaration of Human Rights, 1948.

A recent development of privacy can be seen with the advancement of technology and science which is data privacy. Data privacy is simply to protect all the information that is available on the digital platform with the advent of various legal provisions, acts and especially the EU regulations, known as GDPR the concept of data protection has experienced a positive change. For years, the concept of the concept of data protection was not given much importance but since everything has been digitized and almost all the information is shared, transmitted online across the globe, it becomes pertinent that data protection rules and guidelines are strictly adhered by everyone dealing with the same. Talking about the personal data protection bill of India, undoubtedly it solves almost all the problems and provides various guidelines relating to data privacy and data protection and the same has been inspired by GDPR . With the help of provision of the bill, the way how data is collected and processed can be scrutinized and special emphasis can be given on the safety of the information available. Basically the bill was made so that it can strike a balance between protecting the personal information and data as well as the digital economy. The bill focuses on providing protection to the users with regards to their personal data but there has not been a hundred percent change due to certain exemptions and restrictions. There are various areas where the state's interference is not questioned and this makes it difficult for the complete acceptance of the Bill. There are certain loopholes in the Bill for which many recommendations have been given in various reports.

REPORT SUBMITTED BY JUSTICE B.N SRIKRISHNA COMMITTEE

After the hype created by the Cambridge Analytica case, there were many recommendations and suggestions and many reports were submitted in this regard and the most common and famous one was headed by the Justice B.N Srikrishna and submitted its data framework report to the Government.

HIGHLIGHTS OF THE REPORT:

a) Consent of an Individual- The main clause around which the data privacy and any other information online is based on is the value of consent and it has been recommended that the consent must be lawful and everything that the person consents for must be taken in an appropriate and legitimate manner. The Bill has made the meaning and concept of Consent as the centerpiece of the whole legislation.

b) Data Protection Authority- The formation of the Data Protection Authority is a must and it will be such an authority which will make sure that it will be responsible for the effective implementation of the law. The DPA is bound to perform the following functions:

- Monitoring the legal affairs of the company
- Handling the enquiry and the grievances
- Performing research and awareness programs as and when necessary.

c) Personal Data- The Bill must talk about the personal data of both private as well public entities andthe jurisdiction shall remain with the company if the data has been exercised andprocessed in India . The critically personal data shall fall under the jurisdiction whetheror not it has been processed in the country. All the sensitive personal data including thepasswords, health related details, etc shall be under the scrutiny of the DPA.

d) Data Storage- The provision of data storage deals specifically with the storing of the data in India. It mentions clearly that whatever data is processed and used on the digital platform it must be stored in an appropriate manner. The storing of data is a pre requisite of the data that is supposed to be processed at a later stage.

e) Tribunal and Authorities- The need for an appropriate authority and a tribunal is sine qua non and without a particular authority or a governing power the whole system will be jeopardized. So a need for a tribunal is a must.

f) Penalty- There are many penalties imposed if anyone violates the provisions and breaches the information and the personal data of the individuals. The committee has suggested penalties which are up to 15 crore in certain cases or some percentage of their turnover. The formation of a data protection fund was also asked for and there is a need for the same which will be extremely important for funding out the finances that will be used by the DPA.

g) No retrospective effect- The laws made in the Bill along with all the provisions will not have a retrospective application. They will not be applicable to the previous cases involving the act. The bill will come into force in a systematic and planned manner.

h) Effect on the allied laws- The report has a different effect on the other acts like RTI Act or Adhaar card too because they have an impact on them by mentioning the main objective of protecting the personal data and personal sensitive information. The committee observed that Adhaar Act never spoke about the powers of the UIDAI especially related to the miscreants of the digital world. There is a great need for the amendment in the Aadhaar Act and the government needs to be focused on the provisions of the Act.

Talking about the RTI Act, there are also certain loopholes which must be looked into and the fact that too much information is given to the public might prove wrong and thus the exposure of such sensitive data.

i) Transfer of personal data- The transfers that take place intra country and on a different platform require close scrutiny and a specific legislation and rules. Everything that takes place is through a contract and several

clauses which contain obligations on the part of the transferor that he must follow in order to protect all the violations that might occur in the case of transferee. There are certain prohibitions regarding the cross border transfers and there are some requirements that need to be followed by both the parties.

j) Children's Data- The report has also submitted that there must be specific legislation with regard to the data related to the minors or the children. The companies are up to some extent barred from monitoring and tracking the data that belongs to the children. The main reason and justification for the same is that the children are fully unable to understand the whole process as well as the consequences. The Data Protection Authority is also given a lot of power in handling the data of the children owing to the nature of the children's data and sensitive information. There are other measures taken so as to protect and keep the data and information of the children under some shield so that they are not exposed on the digital platform because they are more prone to the adversities and cyber attacks owing to their tender age.

REFERENCES

BOOKS AND JOURNALS:

- Health Data Privacy Under the GDPR: Big Data Challenges and Regulatory Responses; Maria Tzanou
- Data Protection: A Practical Guide to UK Law; Book by Peter Carey, 2004
- Data Protection and Privacy: The Age of Intelligent Machines, 28 December 2017, Paul De Hert, Serge Gutwirth, Ronald Leenes, Rosamunde van Brakel
- Exploding Data: Reclaiming Our Cyber Security in the Digital Age Book by Michael Chertoff
- Cyber Privacy: Who Has Your Data and Why You Should Care Book by April Falcon Doss
- Customer Data and Privacy: The Insights You Need from Harvard Business Review, 2020.
- The Intelligent Marketer's Guide to Data Privacy: The Impact of Big Data on Customer Trust Book by Kelly D. Martin and Robert W. Palmatier
- Of Privacy and Power: The Transatlantic Struggle Over Freedom and Security; Book by Abraham L. Newman and Henry Farrell
- Data Privacy: Foundations, New Developments and the Big Data Challenge; Book by Vicenç Torra
- Priscilla M. Regan, Legislating Privacy : Technology, Social Values, and Public Policy, 1995, pp.213, 225.

WEBSITES:

- https://searchdatabackup.techtarget.com/definition/data-protection#:~:text=Data%20protection%20is%20the%20process,to%20grow%20at%20unprecedented%20rates
- https://www.techopedia.com/definition/29406/data-protection
- https://gdpr-info.eu/art-4-gdpr/https://www.varonis.com/blog/data-privacy/
- https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html
- https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp
- https://dictionary.cambridge.org/dictionary/english/data-protection

- https://www.collinsdictionary.com/dictionary/english/data-protection
- https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/
- https://blog.netwrix.com/2019/08/08/data-privacy/#:~:text=There%20are%20two%20primary%20types,Examples%20include%20device%20IDs%20orcookies.
- https://www.cleverism.com/lexicon/data-privacy/
- https://www.researchgate.net/publication/258892458_Seven_Types_of_Privacy
- https://www.researchgate.net/publication/258892458_Seven_Types_of_Privacy/link/0c9605295d271f1575000000/downloadfile:///C:/Users/Saumya%20Sharma/Downloads/fulltext-1.pdf
- http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT-D1---final.pdf
- http://webarchive.nationalarchives.gov.uk/+/http://www.dft.gov.uk/consultations/open/
- http://epic.org/privacy/surveillance/spotlight/0605/.
- https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html
- https://gdpr-info.eu/chapter-3/
- https://advisera.com/eugdpracademy/knowledgebase/8-data-subject-rights-according-to-gdpr/
- https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/
- https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/
- https://www.lifelock.com/learn-identity-theft-resources-what-is-data-privacy-and-why-is-it-important.html#:~:text=Why%20is%20data%20privacy%20important,the%20hands%20of%20a%20competitor.
- https://www.analyticsinsight.net/data-privacy-important-comply-regulations/
- https://hyperproof.io/resource/understanding-data-privacy/
- https://medium.com/@neelachary/the-importance-of-data-privacy-39c6676eeb58
- https://blog.eccouncil.org/the-importance-of-data-security-and-privacy-for-businesses/
- https://www.forbes.com/sites/theyec/2019/10/01/10-data-security-risks-that-could-impact-your-company-in-2020/
- http://jagiteservices.com/5-most-common-data-security-threats/
- https://www.endpointprotector.com/blog/top-5-internal-data-security-threats-and-how-to-deal-with-them/
- https://www.sciencedirect.com/topics/computer-science/privacy-threat
- https://digitalguardian.com/blog/insider-outsider-data-security-threats
- https://www.law.com/legaltechnews/2020/06/09/the-increasing-threats-to-data-privacy-and-security-during-the-pandemic/
- https://www.ict4u.net/security/threats.php
- https://mondo.com/common-data-security-threats/
- https://resources.infosecinstitute.com/topic/the-10-largest-privacy-threats-in-2018/
- https://docs.oracle.com/cd/B10501_01/network.920/a96582/overview.htm
- https://www.kaspersky.co.in/resource-center/threats/what-is-cybercrime
- https://searchsecurity.techtarget.com/definition/cybercrime
- https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html
- https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/

- https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook
- https://www.bbc.com/news/technology-54722362
- https://www.indiatoday.in/india/story/what-happened-to-cambridge-analytica-and-facebook-data-theft-case-1712793-2020-08-19
- https://scroll.in/latest/984787/cbi-files-case-against-cambridge-analytica-in-data-breach-scandal-reports
- https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram
- https://m.economictimes.com/news/politics-and-nation/cbi-files-case-against-cambridge-analytica-for-illegal-harvesting-of-facebook-users-data-in-india/articleshow/80400033.cms
- https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3
- https://www.hipb2b.com/blog/two-years-later-cambridge-analytica-and-its-impact-on-data-privacy
- https://epic.org/privacy/facebook/cambridge-analytica/
- https://www.investopedia.com/terms/c/cambridge-analytica.asp
- https://www.crunchbase.com/organization/cambridge-analytica
- https://www.bbc.com/news/technology-54722362
- https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram
- https://www.mondaq.com/india/privacy-protection/1000536/how-serious-is-india-about-personal-data-protection
- http://www.legalserviceindia.com/legal/article-2705-a-critical-analysis-on-data-protection-and-privacy-issues-in-india.html
- https://digitalindia.gov.in/writereaddata/files/6.Data%20Protection%20in%20India.pdfhttps://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf
- https://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pd
- https://iclg.com/practice-areas/data-protection-laws-and-regulations/india
- https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/india
- https://cio.economictimes.indiatimes.com/news/government-policy/indias-first-data-protection-bill-the-road-ahead/72833120
- http://sbj.hnlu.ac.in/digital-age-and-data-protection-laws-in-india
- https://www.barandbench.com/columns/data-protection-regime-in-india-and-compliance
- http://www.rmmagazine.com/2020/03/02/key-features-of-indias-new-data-protection-law/

*****