



COMPREHENSIVE ANALYSIS OF DATA PROTECTION LAWS IN INDIA

Avni Bhargva¹, Dr Kavita Sharma²

5th year BBA.LLB Amity University Noida¹, Professor Amity University Noida²

Abstract : Data protection refers to policies, procedures that protects ones privacy by keeping a check on unauthorized use and dissemination of data . Constitution of India do not explicitly talks about right to privacy , the courts however have from time to time have held right to privacy as part of freedom of speech and expression.

In recent years there have been a significant growth in legislation around data protection the most recent , Digital personal data protection act 2023 : India's first data protection act , which provides for provisions for data storage , data processing , data fiduciaries . The paper will focus on provision and loopholes in IT act , Contract act for protection of data in addition to recent amendments and

DPDP Act 2023 . The paper will also discuss about the regulation enacted by India , the data framework that exist in India for the protection of the data .

Key words : IT Act , Contract Act , Right to privacy , Data fiduciaries , DPDP Act 2023 , European union

Objective of the research : Data in to days time have become an asset , countries have started to frame there own data protection laws to deal to deal with data related fraud and to address the concern related to data protection . With many countries like the European union , which are known for there aggressive stance on data regulation to countries like India which have recently came up with there own data protection law the research object to study in depth the framework that exist how it have evolved along with the loopholes and the case laws that played an important role in the evolution of data protection in the India . Earlier there was no exclusive data protection law in India , however in 2023 India passes DPDA Act 2021 , which exclusively deals with data protection .

Methodology of the research :

The main method used in the research is doctrinal methodology , where existing resources are used for the purpose of the research . Primary resources consist of Digital personal data protection act 2023 bare act , Information technology Act 2000 Bare act , Indian Contract Act . Secondary resources consist of Indian Journal on Advance Sciences , IJRAR E book on the digital era edition 2022 .

The additional method used in research is the comparative methodology . The data protection law of the European Union and the Indian data framework is compared along with this Data protection bill 2006 , 2018 , 2019 are also compared in relation to the scope , the grievance redressal mechanism and the penalties and liabilities .

Introduction and Importance of data:

In today's time data can be compared with the oil and gas , the fossil fuel which every country strive to have the maximum . The Data in layman words can be describes as any kind of figures or numbers or any other kind of information which can be classified or it can be unclassified . Data can be personal like the Sexual orientation of the person ,sensitive like the religious view of the person or the political views of the person which he have kept private and do not want to disclose . Data can be public like the sensenx Index or the nifty index . Before the year 2005 the true potential of data was not realized , the developed countries however gradually started manipulating the data for gaining significant edge over other countries in areas like research and development , strengthening there defense , enhancing technology and fostering research and development . It was European

Union which first came out with its own data protection law after that many countries like the USA and Australia and recently India came out with their law .

Data have a very prominent role to play in almost daily activities of the people . For example if we talk about a body corporate or accompany most of their daily decision are taken based upon the data , the marketing strategy , the recruitment of personnel , analyzing that whether the company decisions are paving way for the rise and profitability is based upon the figures like revenues , expenditure which are kind of a data .

Areas like the health , biotechnology , research and development revolves around data . During Covid pandemic , the need was felt for developing vaccine at a high speed this was possible because of the data . The countries and companies shared among themselves the research data based upon efficiency of vaccine ¹ . Stock market is an another important area where data plays a very crucial role , the strength of the company which is listed in the stock exchange is measured by the investor mainly on the basis of the share price , when the price of the share decreases there is selling of the share and the vice versa .

With the growing technology , there are also concerns about the misuse of the data like cyber threats , people are misusing data to create a fake KYC to avail loans and these kinds of activities can have a bad impact on our economy overall . The data can be manipulated to generate fake numbers or the information when elections are nearby and this can have an adverse effect on the election results also it is an infringement of right to information of the people .

Organizations like the Google and the Apple along with many new technology companies are coming up with their own data centers to harness the power of data . They are opening their big data centers in India which can have a significant economic impact on the countries along with giving enormous revenue generation powers in the hand of the government . Government in India is making it compulsory for companies which have their headquarter abroad to establish their own data centers in India .

Development and origin of data law :

Throughout human history privacy have been important to us . If we look back at the roman period , we will find instances where the using notes of other person or the picture of the person without the consent of that person was considered to be an offence .

With the development of technology and internet the importance of data increased but the crimes and illegal use of data also increased , To cope up with this changes nations started to work on their data laws and came out with there own framework . In the landmark case of **New England life insurance v. Pavesic** ² , the question before the court was whether the individual have the right to privacy , it was held by the court that use of someone's picture without there consent amount to infringement of there right to privacy , the case was landmark event in the further development of data laws . In Roe vs Wade , the USA supreme court held that women has right to undergo abortion and this falls within purview of Right to privacy . The laws and procedures shall be framed keeping in mind the privacy of individual , the women brought the case before the State of Texas and claimed that she have right to undergo abortion , the women was married and pregnant . The court also talked about concepts of social stigma , mental health in its rulings and said that state should consider all this while framing the data laws . Later in US after some years fourteenth amendment was introduced according to which no law which is unfair , not transparent which may lead to infringement of right of public should be introduced in the parliament .

Universal declaration of human rights :

Universal declaration of Human rights in 1948³ was the first time concepts of human rights , dignity and privacy were talked by nations on the global scale . After this declaration developed started framing there own laws on privacy and data protection . Later in 1970 Organization for economic corporation and development which is forum of which various countries are part of came up with its own data regulations guidelines which deals with how data flow can be regulated on global scale , this paved the way for further development of data protections among different developed and developing countries .

European union was the first among the nations to have developed its own data protection law . In 1995 it came with certain directives for data protection . This directives tall about processing , storage and other technical details for regulating the data and enhancing the protection . In 2002 the directives were amended , the scope was enhanced . After in the follow up years there was increase in the use of data for marketing purpose and to regulate it amended European Union communication act . After the landmark cases like wiki leak and the Cambridge analytic a need for exclusive data protection act with stringent measures was

¹ Mary Kay Rizzolo , 12 Reasons why data is important<<https://www.c-q-l.org/wp-content/uploads/2019/12/12-Reasons-Why-Data-Is-Important.pdf>> accessed 04 January 2024

² Pacesich v. New England Life Insurance cooperation [1905] , 122 Ga. 190 ,[50] S.E.

³ Universal Declaration of Human Rights

felt like never before . Finally in year 2018 the European union came out with its own data protection law . The directives were removed and the Act was introduced .

Evolution in Indian context:

In India the formation of data protection framework happened much later in comparison to USA or European Union , this can be traced back to the time when the information technology sector in India was growing at a very fast pace , the companies like Infosys , Wipro , IBM were expanding and establishing their base in India to regulate the misuse of the data , amendment were made in the information technology act 2000 and a clause was added in the information technology act 2000⁴ , Section 43 A was added which says that data can be used only after proper of the individual whose data is being , the sensitive and personal data should be protected with greater security , the section also talks about right to be forgotten principal and provides for the classification of the data . The guidelines and procedures of the IT act were amended in year 2011 and a regulations regarding data transfer , data processing , data transparency were introduced . Earlier Indian law used to have some Data regulation and guidelines for specific sectors like the IT sector , Telecom sector , there were clearly many loopholes and the need was felt for an exclusive data protection law for India .

The evolution of data protection was through many land mark cases that gave brooder interpretation of the Article 21⁵ of the Indian constitution and include the right to privacy in right to life and personal liberty . In the landmark case of Kharak singh v. State of Up , it was the first time the issue of data privacy came before the Indian constitution . The bench of 6 judges was formed by supreme court in this case and it was held by the supreme court that privacy is recognized in Indian constitution , later in the case of MP Singh vs. Satish Sharma the same judgement of kaharak singh vs . state of UP followed and it was held by the bench that US constitution and Indian Constitution are different and we cannot bring the concept of privacy in Indian law . Later in the case of Govind singh v. State of MP the privacy of individual was recognized important and it was held that police should use its investigative power in reasonable manner . Later in the case of Union of India v puttaswamy , judgement in 2017 , a petition was brought by judge in the supreme court , he challenged certain aspects of aadhar card which have become compulsory for Indian citizen to avail various welfare schemes . He challenged the kyc process , certain other details which were availed for aadhar formation . After this Case many attempts were made to introduce to data law many time bills were introduced but were later withdrawn . Finally in the year 2023 India got its own data protection law that is digital personal data protection act .

DATA protection framework in India:

Information technology act 2008

The information technology act or the IT act came into existence in the year 2000 , with the aim to regulate the fast growing information technology sector , later various amendments were introduced to take into account fast growing concerns related to data . A section 72 A was introduced in the information technology sector which talks about data regulation , transfer , transmission and other activities like data storage . In the year 2011 various guidelines were introduced which talked about the handling of the data . It talks about sensitive data , data storage , personal data . Not following the procedure makes the company liable of a fine which can extend to 50,000 rupees .

Another important section which deals with data regulation that was introduced is the section 43 A , which talks about how the company have to maintain transparency and regulations related to data .

Information technology rule came into into existence in the year 2011 , some of the important provisions are-

.It is necessary for the body corporate to take permission of the individual whose data the company intend to use .

. The privacy policy that company brings for its costumer should be in easy language , which is comprehensive . The policy along with guideline shall provide for the purpose for which data will be used , how it will be stored along with the security safeguards and precautions that the company will take to protect to protect the data ⁶.

. The policy shall also contain details about the grievance officer , that the individual can approach in case of any kind of grievance related to his use of data , individual have certain rights over the data even after the data is provided for certain purpose to the company or for any other commercial purpose .

.The details of the grievance officer should be clear and detailed .

⁴ Information technology act 2000

⁵ Constitution of India 1950 ,art 21

⁶ Anirudh Burman , Will a GDPR- style data protection law work for India (2019) (*policy Commons* , 2019)<https://carnegieendowment.org/files/4-17-19_Burman_India_GDPR.pdf> accessed 6 January 2024

. The regulations also talked about the difference between normal and sensitive data . The personal data is the data related to a person medical history , religious view or details like sexual orientation , financial information , which the individual don't intend to make public special precautions shall be taken while handling these kind of the information .

. Section 66 E of the information technology acts talk about a personal liability when he transfer the private images of the person . In that case the person will be liable for fine up to rupees one lakh and also imprisonment .

. Section 72 A informs and impose liability on the body corporate and the individual , when they are under contract and break down the contract related to data privacy .

Sensitive personal data rule 2011 :

The sensitive personal data rule or the information rule 2011 were introduced with the objective to protect the sensitive data and provide additional security and safeguards for the sensitive , the sensitive can be medical reports , financial information , password or any kind of data which relates to the personal directly or in indirect manner and the individual wants to keep private . This sensitive personal data rule 2011 intends to protect sensitive data but do not impose any kind of liability when the safeguards are not followed by the body corporates .

Intermediary Guidelines and Digital Media Ethics, 2021:

The guidelines were introduced in the year 2011 to broaden the existing framework for data protection and make the publisher of the data and the intermediary liable .

The intermediary in todays time have even more role to play in the data regulation relative to the content producer . The intermediary are the one who connect customer to the content creator and play important role in decimation of information and data .

Some of the guideline are –

The intermediaries shall provide there privacy policy to the customer , it should be clear on several aspects like the kind of security safeguards that they will provide along with the responsibility of the intermediaries and the responsibility of the customer .

Necessary amendments and changes shall made in there policy from time to time , and the customer through email .

The customer shall be informed as soon as possible for any kind of suspicious activity , and the intermediary shall cooperate with the government security and investigative activities .

The grievance officer shall keep the customer aware about the complaint that a customer have filed .

DATA PROTECTION BILL 2006 , 2018 AND 2019:

The growing pace of technology made it necessary for India to have its exclusive data protection framework and the in the year 2006⁷ finally India came with its own data protection framework

Some of the features that were introduced are –

.It imposes criminal and civil liability upon the individual who do not comply with the guidelines and the process and provides for fine which can extend up to three lakh rupees⁸ .

. Also with providing certain exemptions to government for certain purpose it also impose certain liability on government like not disclosing the data and keeping the data of public safe and secure .

. The bill provides for data protection body that will be formed which will provide for dispute resolution related to data protection and its decision can be appealed before high court .

. The bill highlights the relevance of the consent and says that relevance is important when it comes to using data for any kind of commercial or any other activity .

The bill however failed to receive the consent of the president .

⁷ Data protection Bill , 2006

⁸ Shiv Shankar singh , Privacy and data protection in India : a critical assessment , *Journal of the Indian Law Institute* (2011)

<<https://www.jstor.org/stable/45148583>>assessed 1 February 2024

Srikrishnan committee was formed to introduced to take consideration various stakeholder on the basis of the recommendation of the committee data bill 2018 was brought forth but was altered withdrawn in the similar data protection bill 219 also didn't received the assent .

Digital personal data protection act 2023

Bill highlights :

Applicability - The applicability of the bill extend to the data which is stored and processed in India , the bill extends to the data which is in digital format but is collected offline . The applicability of the bill extends to outside India in case the body corporate is giving services to the customer in India . The term processing of the data means the operation which is done on the data . It can include use , sharing ,collection .

Rights of the principal - The individual whose data is shared , used , collected or operated is known as principal . The principal will have various rights – Seek grievance redressal , Modify or correct the consent that was given , right to have an nominee who can exercise rights on their behalf .

Data principals will also duties like – To not file a false complain . IF the data principal do not follow the duties which are given in the digital personal data protection act 2023⁹ , it can be punishable offence .

Consent- The consent plays a very important part in determining the rights and infringement . If before processing the data the necessary consent was taken it will be not considered infringement and if the consent was not taken or if data is used for any other purpose other than the purpose for which the consent was obtained it will not constitute to be an infringement . Consent will not be required in few cases like the medical cases , government purposes like investigating crime , the data is collected by employer for some legitimate purpose , the data is voluntary given by the person for certain use like for example for an educational survey .

Data fiduciaries –Data fiduciaries is a kind of intermediaries that determine how the data will be processed , how will it be used . The DPDP act enlist certain obligations of data fiduciaries like - Making sure to develop safeguard and safety around data , Making sure that is complete and accurate , The data protection board shall be informed from time to time about the possible infringement cases or any kind of security threat from the data . Data fiduciaries¹⁰ have right to transfer to any place outside except certain places restricted by the government .

Exemptions - The data fiduciaries will not have certain rights and duties in certain cases like government investigation , public order or the defense purpose .

Penalties – The bill provide penalties which are more stringent as compared to the previous bill like the fine in the case of data violation related to children can extend up to 200 crore . If the data fiduciaries or the entity fails to take the required action , the company will be liable to fine which can extend till 250 crore .

Issues with the digital personal data protection act :

Like the previous data bill , the digital personal data protection act 2023 contain certain loopholes like it gives much power in the hands of the state or the government in name of defence , security or the public order and it can lead to severe infringement of the rights by the local government bodies and infringement of the privacy of the citizen , the government can store data in the way it want and for the time frame it want and there are no deadlines regarding this . The data fiduciaries are given warrant by the government for the time period government think fit to not comply with the rights and obligations it may deem fit . Supreme court in is order in the year 1996 brought certain guidelines which imposes certain restriction like the storage or transfer limits however while framing this bill that guidelines were not taken into account also the considerations of srikrishna committee regarding restricting the powers of the government were not taken into consideration . It was held that such restriction on the power will be done through other act . For certain purposes like the welfare of the state , for certain schemes and for the purpose of license and certificate , the consent of the individual is not required and the state is free to use the data , the provision is totally overridden by the bill for these purposes and the purpose limitation is also not imposes which is to use the data for specific purpose .

Personal data – The bill does not talk about personal data , in the srikrishna committee and the previous data bill like the 2018¹¹ 2019¹² , 2006 data bill the personal data was something which was given special reference , the personal can have serious implications on the individual like the mental health , reputation damage , financial loss . The srikrishna committee , General data

⁹ Digital Personal Data Protection Act , 2023

¹⁰ A Dobklin , Information fiduciaries: Data privacy and user expectation in Practice , 2018 (*Technology law Journal*)<<https://www.jstor.org/stable/26490153>> Assessed on 2 January 2024

¹¹ Data protection bill , 2018

¹² Data protection bill , 2019

protection regulation of European Union regulates the use of personal data very stringently unlike the Indian digital personal data protection act 2023 .

Right to be forgotten- It is the right of the individual or data principal to limit their personal data use or disclosure . This is not provided

Right to data portability – It the right of the data principal to transfer the data from data fiduciaries to the some other place . This is another important right that is not provided .

No stringent protection and regulation on transfer of data to other countries , this is a very pressing issue the bill provides for the transfer of data to any countries unless it is not exempted by the notification of the government . This creates question mark upon the adequacy of protection as once the data leaves the jurisdiction of India it is not in the hand of the government to regulate it .

Shot tenure of the members of the data protection board is also concerning since it lowers the efficiency and working of the board.

Protections and regulation in case of cross- border transfer- The act gives the power to the government to restrict the countries where it can transfer data this can be done through notification . Through this powers to central government the privacy and rights of Indian individual over there data can be protected and the countries where there are no safeguards for data protection the data will be not sent in those countries , as the Indian law jurisdiction will not extend to those countries and there is no control over how the data will be used .

Data Board provisions – The act provides for the establishment of data board but the tenure of the members of the board is restricted till 2 years , which is very short and have to be ideally for 5years . The reappointment of the members of the board is allowed . This will the working of the board and also efficiency . The board will serve some important functions like investigating cases related to data infringement , monitor the compliance of the rules and regulations which are mentioned in the data protection act 2023 . The decisions of the board can be appealed before the appropriate board and . Supreme court in 2019 mentioned that the tenure of the members of the data board only for 2 years along with the provision for reelection will increase the influence and interference of the executive over the legislature . Bodies such as competition commission of India and other tribunals also have five years term.

Provisions related to childrens – The data provisions related to childrens are more stringent as compared to other provisions . In the act the age of children is below 18 , the saikrishna committee also recommended the age of children as someone between 18 to 13 , as in the countries like UK children have been defines as the person below 13 years of age . In India the children are the individuals below 18 years of age , and this is applicable for any matter related to digital personal data protection act 2023 ¹³. The saikrishna also recommended that the age of 18 years is too high and the children should be someone below 18 years somewhere around 15 years to make decisions related to data usage , however in other acts like the Indian contract the children is an individual who is below 18 year , to avoid any contradiction, in the digital personal data protection act 2023 the child age have been defined 18 .

For the purpose of safety and safeguards for the children the data fiduciaries or any intermediary who is dealing with data related to child should obtain the consent of the legal guardian , however this provision may lead to interference of the privacy that is the reason it was recommended by the srikrishna committee to keep the age as low as possible . Also there are a lot of compliance problems in this procedure , the child might give the fake details of the parents or the guardian and following the process will become difficult , the object to protect child data just by obtaining the details of the guardian is not effective enough to protect the child from digital and technology threats like cyber bullying , sexual harassment and other kinds of the crime in the online world . The act says that necessary safeguards shall be taken for the purpose of the protection of the children by the data fiduciaries but does not mention about the exact safeguard that needs to be taken , this creates anonymous conditions and leave it the intermediary on how they feel to go about the safety and precautions related to child data . The act gives certain powers to the government to provide exemptions to the startups and certain companies to not follow the consent mechanism and procedure if certain conditions are fulfilled like data is procured in large volume , in that the company or the entity may not disclose the purpose for which the data is obtained and other details ¹⁴.

¹³ M J Ghosh , U Shankar , Privacy and data Protection Laws in India : A right based Analysis , *Bharati Law review* (2016)<<https://www.academia.edu/download/59185035/BhartiLawReviewPaper20190509-129316-1q1f8xg.pdf>> last accessed on 6 January 2024

¹⁴ N Sundera , N Narendaran , The Digital personal Data protection Act 2023 : Understanding India's Dyanimic approach to data protection (*Computer law Review International*) < <https://www.degruyter.com/document/doi/10.9785/cr-2023-240502/html>>, Last accessed 20 January 2023

Land mark cases :

-People union of civil liberty vs Union India

In this case a petition was filed by the person against central bureau of investigation , a phone call of the person was tapped without the consent of that person , it was argued by the petitioner that it was violation of his rights under article 21 of the constitution that is right to life and personal liberty . The decision of the court was in the favor of the individual and it was held that taping the phone call without the consent of the individual is the infringement of the right of the individual and the violation of the privacy .

-R. Rajagopal v .state of Tamil Nadu

This case is famously is auto Shankar case . The petitioner argued that the prisoner in the jail shall be allowed to right his auto biography and publish it , there shall be no restriction on this as it is his inherent right under article 21 . The court gave the decision in the favour of petitioner and held that the right to write autobiography and publish it is covered under right to privacy and cannot be taken away .

- KS Puttaswamy v Union of India ¹⁵

The decision was given in the year 2018 by a bench of 9 judges . Article 21 that is right to life and personal was interpreted to include right to privacy within it . The court held the following

. The right to privacy is already included in the constitution of India . Privacy also includes a important right that is right to be left alone . The liberal of the constitution is necessary . There are restrictions on the usage of one's data and proper consent is necessary .

Results of the Research :

India is working for the betterment of data protection and right to privacy . In 2023 it came out with digital personal data protection act 2023 . However there are still many issues that remain unaddressed.

The data protection board is not efficient in its functioning , because of this grievance is not redressed properly . The government has been given many power in the name of public order , morality which may be misused .

There is lack of awareness among citizen in respect of importance of data and the government should make more efforts to educate and raise awareness about data protection . The proper implementation of data protection act is necessary . While framing laws around data protection it is necessary to take caution that it does not hamper creativity and development as the new startups are mostly dependent upon the data that already exist in the market .

¹⁵ KS Puttaswamy and Anr vs Union of India ; (2017) 10 SSC 1