THE DIGITAL PERSONAL DATA PROTECTION ACT OF 2023: STRENGTHENING PRIVACY IN THE DIGITAL AGE

Shubham Saurabh, Gujarat National Law University

ABSTRACT

The Digital Personal Data Protection Act of 2023 stands out as a crucial legislative milestone in preserving individual privacy rights and strengthening data security in a time of unprecedented data generation and consumption. This in-depth analysis explores the main clauses, ramifications, and difficulties brought on by this historic law.

This study examines the fundamental ideas behind the Act, emphasizing its dedication to giving people more power over their personal data. It examines the complex processes of consent, data minimization, and the right to be forgotten, shedding light on how these provisions redefine the relationship between people and the companies that gather their data.

The research also closely examines how the Act will affect businesses and organizations in terms of compliance and operational changes. The obligations imposed on data controllers and processors are broken down, highlighting the necessity of effective data protection frameworks and procedures.

While the Act offers the establishment of the Data Protection Board of India, which will be the Central Watchdog for the protection of personal data being misused by big data collectors.

Additionally, this study critically evaluates the Act's enforcement mechanisms, assessing the role of regulatory authorities, penalties for non-compliance, and the potential impact on global data flows and international data governance.

As society marches further into a data-driven world, the Digital Personal Data Protection Act of 2023, serves as a beacon for privacy rights and data protection. This analysis offers insightful information about the Act's significance, its effects on people, groups, and society at large, as well as how it will affect the future of the digital landscape.

Keywords: Digital Personal Data, Data Security, Data Fiduciary, Right to be Forgotten, Data Consumption, Governance.

INTRODUCTION

Personal Data, is an inherent and inalienable characteristics of human being. It speaks about that individual, how he/she will be recognized in a society.[1] This can be anything which links to that person or individual that helps in identifying that person is his personal data. This can be name, surname, email address, phone number, or even your choices regarding any book, food, political ideologies etc. This makes the personal data, the most vulnerable thing in this digital era. Companies as well as that process these personal data usually provide their services free of cost. This processing of personal data helps in understanding human behaviour, tastes patterns about that particular individual, which helps them to create targeted ads that they can sell and generate revenue. The unchecked or unregulated processing of these personal data may have a dire or unpredicted results which not only violate the basic fundamental "right to privacy"[2] of that individual guaranteed under "Article 21 of the Constitution of India"[3], but also shows the inability, incompetency or lack of government will to protect the fundamental rights of their citizen.[4] The idea of data protection has roots in several different nations. The European Union law i.e General Data Protection Regulation is one such law which can be the champion in data protection all around the world.

The enactment of law for regulating this personal data protection is a complex exercise which requires a careful approach to balance the privacy concern at one hand and legitimate State interest at the other hand.[5] In order to make the reality of landmark judgment of the Supreme Court of India in "Justice K.S. Puttaswamy (Retd) v. Union of India"[6], "the Digital Personal Data Protection Act, 2023" was enacted by the government on 11th August, 2023. The fundamental idea behind this was to recognise both the "right of individual to protect their personal data" and "the need to process such personal data for lawful and legitimate purposes."[7]

The Act applicable to the administration of digital personal data across India, whether obtained via the internet or otherwise. There are some exemptions given in the Act as well like data processing by the instrumentalities of the State such as national security. The Act does not even

[1] "Prakash Shah, *International human Rights: A perspective from India,* 1 FORDHAM INTERNATIONAL LAW JOURNAL, 24, 24-28 (1997)."
[2] "Justice K.S Puttaswamy (Retd) v. Union of India, (2017) 1 SCC 10"
[3] INDIA CONST, art.21, cl.1.
[4] Puttaswamy(Retd), 10 SCC at 56
[5] Puttaswamy(Retd), 10 SCC at 58
[6] Puttaswamy(Retd), 10 SCC at 127
[7] "The Digital Personal Data Protection Act, 2023, Object, No. 22, Acts of Parliament, (India)"

recognizes the consequences or harms arising from processing of personally identifiable information. Right to be removed (forgotten), principle of consent, Data Protection Board of India are some of the key component or highlights where it is helpful in understanding the function measures taken by the government to control the illicit use of personal data by data fiduciaries.

One another key component that makes this Act a major boost for strengthening the right to privacy is the amount of penalty that may be imposed on data fiduciaries if they are found guilty of violating the provisions of this Act.

Before this Act, India does not has any stand-alone legislation that talks about the data protection. The recognition of personal data as a "right to privacy" necessitates the urgency for having a separate law for regulating the processing of personal data especially in digital platform. The work on this Act began nearly a years after the Puttaswamy, when the union government established a expert committee on Data Protection, chaired by Justice B.N Srikrishna, to review and explore data protection problems and difficulties in our nation-state. In July 2018, the committee present its report. The Personal Data Protection Bill, 2019 was introduced in Lok Sabha in December 2019 at the Committee's proposal,[8] the bill was later withdrawn from Parliament due to report submitted by Joint Parliamentary Committee. Then bill was released for public opinion in November 2023.[9] The Digital Personal Data Protection Bill, 2023 was reintroduced into Parliament in August 2023 and got its assent by the President on 11th August 2023.[10]

Data Processing of personal data in digital realm will only be done through the letters of this Act and obviously for lawful and legit purpose. This research paper will try to examine the power given to people over their personal data, process of consent, right to be forgotten, impact on business and organisation in terms of compliance and operational changes, obligation on data controllers, "data protection board of India," penalties for non-compliance. The data protection is the authority for the "right to privacy."[11]

[8] Pre Legislative Research, https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023 (Last visited Oct 5, 2023)
[9] *id*
[10] *See Supra note 8*
[11] "LEE A. BYGRAVE, PRIVACY AND DATA PROTECTION IN AN INTERNATIONAL PERSPECTIVE 165-200, (Stockholm Institute for Scandinavian Law 2nd ed., 2010)."

RIGHT TO PRIVACY AND DATA PROTECTION

When the United States' East Coast had seen unusually intensive urbanization, Warren and Brandeis formulated the concept of the right to privacy. The period between 1790 and 1890 witnessed a rise of the US population from 4millio to 63million. More than 8 million people had immigrated to the US by 1890. Rapid technological advancement and innovation have put pressure on the private sphere and being under stress.[12] "The right to privacy" is a part of human dignity and guarantees that a person can live with dignity by protecting the private information of their personality from unauthorized access. Individual autonomy and freedom to make crucial decisions that have an impact on one's life are both recognized by privacy. This postulates the reservation of a private space for the individual, described as the right to be let alone. Every person is born with the inherent right to privacy, which is essentially a natural right. Such a right belongs to every human being till the last breath is taken. It does go hand in hand with human beings and is unalienable from them. It emerges from the human body and dies with the human body.[13]

The "right to privacy" in the digital sphere can be preserved by the way of data protection. The concepts of privacy and data protection are intertwined historically. At the most fundamental level, data protection is largely predicated on how Article 8 of the European Convention on Human Rights is interpreted, but in practice, these two rights are still muddled. Moving from what sets the right to data protection apart from the right to privacy seems like a good place to start when trying to define the essence and justification of the right to data protection.[14]

Between data protection and the right to privacy, there is one key distinction. By referencing their role within the constitutional state, this distinction is made on teleological grounds. The right to privacy is a "tool of opacity" that shields people from government and private actors' intrusion by forcing them to refrain from unwanted action. By establishing normative boundaries for it, privacy restricts authority. On the other hand, data protection primarily serves as a "tool of transparency," regulating and channelling the exercise of power rather than putting

[12] "Samuel D. Warren And Louis D. Brandeis, *The Right To Privacy,* 4 HARVARD LAW REVIEW (HLV) 193, 193 (1890)."
[13] *See supra* note 2 at 134.
[14] "F. FABBRINI, FUNDAMENTAL RIGHTS IN EUROPE: CHALLENGES AND TRANSFORMATIONS IN COMPARATIVE PERSPECTIVE 319 (Oxford University Press 19th ed., 2014)."

a stop to it.[15]

CONCEPT OF PERSONAL DATA

"Personal Data"[16] is any piece of information that is connected to an "identified or identifiable living individual".[17] This can be scattered pieces of data which may be joined together and then result to the determination of a specific person and the creation of private information. Personal data that is completely anonymous in that way which is no longer useful to identify a person is no a personal data. The definition given under the Act is very precise in determining any data as personal data. Designation, surname, place of residence, email, identification card number (AADHAR NUMBER), mobile number, Internet Protocol address (IP), and so on are some basic illustrations of "Personal data". The prime motive of this Act is to safeguard these data's from being misused by any data processing entity. But the law is helpless in a case when your personal data is publically available and with your consent as well. Let's take a hypothetical situation Mr. A is an individual who makes video content for any digital platform say for example X and in doing so Mr. A negligently or carelessly disclosed his personal details like his home address or email address. Then in this situation Mr A can't claim or seek the protection of this law that he is being spammed by any particular company over his email address.[18] The general notion among citizens is that once the law is there no one can use their personal data but the thing is their data is being used, processed by those data processing companies because their personal data's are publically available to those company and they don't need you consent in this situation to process those data for their benefit. To avoid these kind of situation one always need to be careful and vigilant on digital space about whatever he/she is posting and how it is related to their personal data.

COMPONENTS OF CONSENT

Consent is the basic aspect of human interaction, it gives an autonomy to an individual over

[15] "Bart van der Sloot, *Privacy as Personality Right: Why the ECiHR's focus on Ulterior Interests Might Prove Indispensable in the Age of 'Big Data,* 31 UTRECHT JOURNAL OF INTERNATIONAL AND EUROPEAN LAW 25, 28 (2015). *See also,* There is, undeniably, 'a strong tendency in case law and literature to understand privacy as a broadly conceived concept of autonomy and information autonomy of the human person': Paul De Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in Erik Clases, Antony Duff and Serge Gutwirth (eds), Privacy and the Criminal Law (Intersentia, 2006), 61."

[16] "The Digital Personal Data Protection Act, 2023, § 2(t), No. 22, Acts of Parliament, (India)"

[17] *id*

[18] "The Digital Personal Data Protection Act, 2023, § 3(c), No. 22, Acts of Parliament, (India)"

his rights that can be exercised by him/her like natural rights, fundamental rights, statutory rights, customary rights etc.[19] This protects the individuality of a person that makes him/her different from others.[20] Consent helps to recognise the will, that a person exercises from its own and this needs to be protected rather it is the responsibility of the State to safeguard the consent of its citizen. In that light various components of consent have been integrated in the Act, some of the major elements of Consent are:

1. Consent must be without duress, exact, informed, without conditions and incontestable and limited to such purpose only for which consent was given.[21]

2. Consent infringing the letters of any law shall not be a consent at all.[22]

3. Every consent form presented to individual (Data Principal)[23] be in clear, plain and in that language understandable by the individual, together with the particulars of "Data Protection Officer".[24]

4. Withdrawal of consent shall be as easy as when the consent was taken. (Right to withdrawal of consent).[25]

5. Consequence of withdrawal shall lie upon the individual itself.[26]

6. The burden to prove that consent was taken for processing the personal data shall lie upon the Data Fiduciary.[27]

The above components of the consent clearly empower the data principal over his/her personal data. It gives immense authority ranging from the manner to get consent to burden to prove that consent was taken as per the provisions of the law. These component strengthen the overall

[19] Schuck, P. H., *Rethinking Informed Consent*, 103(4) The Yale Law Journal (YLJ) 899, 915 (1994), https://doi.org/10.2307/797066(1994).
[20]"Carpenter, B., O'Brien, E., Hayes, S., & Death, J., *Harm, Responsibility, Age, and Consent*, 17(1) New Criminal Law Review: An International and Interdisciplinary Journal, 23, 23–54. (2014), https://doi.org/10.1525/nclr.2014.17.1.23."
[21] "The Digital Personal Data Protection Act, 2023, § 6(1), No. 22, Acts of Parliament, (India)"
[22] *Id.* § 6(2) *note 21*
[23] Id § 6(3) note 21; *See also,* Data Principal means the individual to whom the personal data relates.
[24]*id*, § 6(3) note 21; "Data Protection Officer means an individual appointed by the Significant Data Fiduciary" § 2(i); "Significant Data Fiduciary means any Data Fiduciary as may be notified by the Central government" § 2(z)
[25] *id* § 6(4) note 21.
[26] *Id* § 6(5) note 21
[27] *Id* § 6(10) note 21;*See also "*Data Fiduciary means any person alone or in conjunction with other person determine the purpose and means of processing of personal data."

privacy of individual over his/her personal data in digital space. This put extra burden on the part of data fiduciary to make themselves aware about the compliance of this law or else face severe consequences.

"RIGHT AND DUTIES OF DATA PRINCIPAL"

"Data Principal" are the person whose personal data is being collected, stored, and processed by the Data Fiduciary to offer their services. The components of consent clearly shows the value of personal data and autonomy given to data principal in respect of his/her personal data. It is as if "my data my will" and this also helps in strengthening the overall pillars of right to privacy. But apart from all these there are certain sets of rights and duties that the data principal must know before granting his/her consent to process personal data. First let us understand the rights that are available to data principal.

- **Right to inspect about private information.**

Data principals are given the right to inspect their private information he/she has originally given consent for processing. Data principal can get summary of private information, details of all other "data fiduciaries" and "data processors" with whom the private information was shared, any other information which may directly or indirectly related to that personal data.[28]

- **Right to rectify and deletion of "personal data"**

Individual or Data Principal being the sole owner of their personal data gives them the undisputed authority to check whether the shared data received by the data processor is correct or not. In case if the said information is not correct and not giving the complete idea about the individual then person shall have all the right to rectify those collected data. Data processor shall on the demand of individual either edit the wrong or misleading data and correct the incorrect data or update the private data.[29]

Even individual shall have a power to get it deleted from the database of data processor, the company or organisation shall within a reasonable amount of time delete those information. This right strengthens individuals to have control over their personal information, ensuring that

[28] DPDP Act 2023, § 11
[29] DPDP Act 2023, § 12

it is not only accurate but also kept in line with their current preferences and consent. Organizations handling personal data are statutorily bound to respect and facilitate these rights, enhancing individuals' privacy and data protection in an increasingly digital world.

- **Right of grievance redressal.**

This right enhances the mechanism adopted in the Act by putting extra obligation on data fiduciary to be available to register any grievance by data principal. The company or organisation through its appointed official must respond to any of the issues in time bound manner which may be prescribed with passage of time. It is duty of Data principal to exhaust all the rights of grievance redressal mechanism offered by the data fiduciary before approaching the Data Protection Board of India.[30]

This may increase the time to get the things done for aggrieved data principal but this also has an advantage as it help to solve the issues of at preliminary level only and data principal will get exempted from rigorous mechanism of law to get thing sorted. It is a two way sword for both for the individual as well as the data processor.

- **Right to nominate**

This right helps the individual to secure their data in case he/she is not able to make decision because of any unforeseen event. Data principal can nominate any other individual who will be solely responsible to take decision in terms of data of that person.[31]

This ensures that an individual can specify a trusted person or entity who will have the power to make decisions or receive the perks on their behalf if they are unable to do so by themselves. This is as if the power of attorney given in case of sale of immovable property where the owner appoint any person as power of attorney who shall exercise all the duties on behalf of the owner, but there is slight difference in both the concepts as in power of attorney the owner is able to do all those thing that the person appointed will do but in case of nomination the data principal must be in a situation where he/she is not able to exercise his mind over the personal data.

[30] DPDP Act 2023, § 13
[31] DPDP Act 2023, § 14

All these above points gives right to data principal over his/her personal data, now let us see some of the general duties that he/she must be vigilant while exercising the protection of law at the same time. The duties enshrined under the Act are:

- Be in boundary of law while exercise the right over personal data as no one is above the law.[32]

- Not to impersonate any other person over digital space because impersonation is a criminal offence under penal laws of the country.[33]

- Not to conceal the significant information while providing the personal information like duplicating the identity proof of address issues by appropriate authority.[34]

- Avoid to file any unnecessary complaint with "Data fiduciary" or "Board".[35]

- To show or produce only true and authentic data while exercising the right to rectification or deletion under the law.[36]

OBLIGATION OF DATA FIDUCIARY

Data fiduciaries are those entities who are primarily responsible for collecting, storing, processing of data. The Act puts some obligation that these entities have to follow in order to avoid any penalties from the Data Protection Board of India. These obligation are somewhat duties which they are abide to follow. The nature of this obligation is such that even if there is not any agreement between Data Principal and Data Fiduciary, Data fiduciary be responsible to follow the letters of this law or any regulation made or prescribed whenever they are processing personal data of the individual. Some the key obligation of these entity are listed below:

- Any Data Fiduciary which is engaged or involved in Data processing of personal data in order to offer any goods or services to that person shall do it only under a valid

[32] DPDP Act 2023, § 15(a)
[33] *Id* § 15(b) note 32
[34] *Id* § 15 (c) note 32
[35] *Id* § 15(d) note 32
[36] *Id* § 15(e) note 32.

contract.[37]

This means there must be a valid contract for data processing of personal data between individual and data processer. Let's assume an insurance company X offering services of life insurance to their clients, then that company must have personal data of many of their clients, in order to process those data there must be a valid contract between the insurance company X and its clients. The contract must clearly mention the terms, motive for which personal details are getting grinded by the company.

- If company or organisation is taking any decision that will ultimately affect the data principal or going to disclose the personal data to another data fiduciary then in that case data processer must ensure its authenticity, precision and persistency of the private details.[38]

Let me put this in another way imagine a person name Ram who applies for a loan on an online lending platform. The platform acting as a Data fiduciary, collects and processes Ram's personal data, including his financial history, employment details and credit score. The online lending platform uses Ram's personal data to assess his creditworthiness and decide whether to approve the loan application or not. This decision significantly affects Ram as it will help him to get loan which might be critical for him. In such situation the lending platform is duty bound to produce the personal details in complete, exact, and consistence with that of Ram.

- The organisation must protect the private details in its holding or under its authority.[39]

- Entity must implement a reasonable security measures to prevent any breach of data from its possession.[40]

- Even after taking all the security measures the data breach of personal data occurred then it shall be the duty of data fiduciary to intimate such breach of information to the data principal. The intimation information letter must cover the data that is breached

[37] DPDP Act 2023, § 8(2)
[38] *Id* § 8(3) note 37
[39] *id* § 8(5) note 37
[40] *id*

and how it affect the data principal as well.[41]

- Duty to erasure the personal data within reasonable period of when the purpose for which data was collected or data principal has withdrawn the previous given consent.[42]

- Must appoint an individual who will be the sole point of touch between data fiduciary and data principal.[43]

- Must implement an effective grievance redressed mechanism for data principal.[44]

Apart from these general obligations upon Data fiduciary, central government on the assessment of any other factor put some additional obligation on significant data fiduciary. This may include independent data auditor to shall be responsible to perform the data auditing[45] and analyse the adherence mechanism of "Significant Data Fiduciary."

"DATA PROTECTION BOARD OF INDIA"[46]

The Data Protection Board of India (DPBI) is a regulatory body which would be set-up at appropriate place where the union government thinks fit. This body corporate comprise of chairperson and members appointed by the Central government. The Board holds a significant and central role for compliance of DPDP. It can direct urgent measures that shall be taken in case of personal data breach, investigate the breach itself and impose appropriate fine. It can also issue suitable directions. Any appeal against the order, direction can be preferred before "Telecom Disputes Settlement and Appellate Tribunal (TDSAT)"[47] within 60days, and an appeal challenging the order of TDSAT lie only before Supreme Court of India.

DPBI has been given the authority to levy a huge monetary penalty of up to Rs. 250 crores. It will have to contemplate the seriousness, magnitude, timeline, repetitive nature of such breach, the kind and category of the private details in question, unlawful gain in committing such

[41] *Id* § 8(6) note 37
[42] *Id* § 8(7) note 37
[43] *Id* § 8(8) note 37
[44] *id*
[45] DPDP Act 2023, § § (10)(2)(b)
[46] DPDP Act 2023 § 18
[47]DPDP Act 2023 § 29(8); *See also,* "Telecom Regulatory Authority of India Act, 1997" § 14A & § 16, No. 24, Acts of Parliament, (India).

breach and so on while deciding the quantum of monetary compensation to be imposed.

Having a separate body that will be responsible for regulating the breach of personal data gives in-depth understanding and helps in taking informed decision. A independent board can solely concentrate on this problem and try to solve the problems associated with data breaches. This also helps in reducing the time for data principal to secure their personal data and prompt action is possible. Specialized boards are often more open to innovation and new approaches in addressing issues. Their specific focus allows them to explore creative solutions and adapt to evolving technologies and trends in data protection.

IMPACT ON BUSINESS AND ORGANISATION IN TERMS OF COMPLIANCE AND OPERATIONAL CHANGES

The enacted of DPDP Act, 2023 will made a revolution in future in terms of protecting the personal data and upholding the right to privacy enshrined under Article 21. This Act will impact the data processor significantly in terms of its compliance and made them to change in their operational framework at the same time. These operational framework will hurt their business activities, services and other fundamental elements of their activities. Some of the major impacts are as below:

1. Establishment of Data Protection grievance redressal mechanism.[48]

The Data Fiduciaries have been statutorily mandated to establish a grievance redressal mechanism, which will serve data principal in lodging their grievances in the form of compliant if they found that their personal data is being misused, altered or used for any other purpose for which it was collected.

There must be "Data Protection Officer (DPO)" who shall be appointed by the business or organisation. The contact details of DPO will be publically available. DPO shall be the only point of contact between Data Principal and Data fiduciary. DPO will respond to all the lodged complaint within prescribe period of time and ensure the effective resolution of issues faced by the data principal. The basic idea or purpose for having a separate individual is to ensure accountability and transparency on the part of data processor.

[48] *See supra* note at 30, 44

2. Executing Independent Data audit.[49]

Executing an independent data audit is a important process to analyse, evaluate and enhance the organisational data protection mechanism. This process helps in designing a robust system that will ensure accurate and efficient information of data principal. The audit involves a regular examination of data management process, data sharing and data usage within data processor. The purpose is to identify lapses vulnerabilities, area for improvement and compliance of DPDP Act, 2023.

The audit would involve interview with key personal, involved in data management, IT staff and Data Protection Officer. These discussion may help auditors to gain real situation of organisational data handling processes regarding personal data protection practices.

After the assessment, the data audit team will prepare a detailed report. The report will state the strength and weakness of organisation and recommend the area for improvement.

3. Keeping accurate personal data.[50]

The legal obligation of organisation to ensure true and accurate personal data of data principal put extra burden on data processor. This means that business or organisation must take appropriate steps to verify data, regularly updates, cross verification, error correction and providing access to data principal.

4. Ensure Informational Privacy.[51]

Ensuring an informational privacy in digital age is utopia but trying to reduce the same is not an impossible task at the same. This gives safeguard to individual sensitive information from unauthorized access. Achieving these require business and organisation to implement a stringent security measures, robust encryption protocols, and access controls within data processor structure. Strict adherence to DPDP Act, 2023 require an organisation to educate their employees and provide them clear instruction about how the collected personal data be used in well-defined manner. Regular data audits, risk assessment, and prompt response to data breaches are essential to ensure a effective mechanism for informational privacy. These things

[49] *See supra* note at 45
[50] *See supra* note at 38
[51] *See supra* note at 40

will certainly affect entities in their operational cost, it will be interesting to see, how they will manage their cost to keep offering free services to their customers.

5. Facilitate right to access of information[52]

Facilitating the right to access information under the "Digital Personal Data Protection Act, 2023" means ensuring the individual to have easy access to his/her personal data stored by the data processor. Individual being the owner of his/her private details has all the right under the Act to know what information organisation have collected about him and for what purpose and how it will be used and with whom the data fiduciary is sharing such data. To offer all these facilities the business organisation are obligated to establish a mechanism such as online portals or dedicated customer service channels, enabling data principal to request for their data. They can even withdraw the consent given to store the data and data fiduciary have to delete all those collected data within a reasonable period of time from their databases.

6. Facilitate state instrumentalities in discharging public function.

It shall be the duty of Data Fiduciary to help the state agencies in discharging their public function. Central government may even ask to stop the transfer of personal data to outside India. This will surely impact the core business activity of data processor because their main function is being stopped here. Adjudicating body specially entrusted may direct these company or organisation handling personal details, to furnish them before their clients and they are duty bound to furnish all such data. They can't deny stating that this will go against their privacy policy. Personal data may be asked by state agencies in the pursuit of preventing, identifying, probing or pursuing legal action against any violation or breach of the law. The general ground upon which State and its agencies can process the personal data violating the fundamental right to privacy in safeguarding the India's sovereignty and integrity, ensuring state security, fostering amicable relationships with foreign nations, preserving public order, and averting provocation leading to any recognizable offense, etc.

CONCLUSION

In the multifaceted landscape of digital world, the importance of data protection and privacy has never been more crucial than it is today, where data flows continuously and technology

[52] *See supra* note at 28

manages every area of our lives. Data protection and privacy now emerged as the fundamental rights. The debate over these topics highlights the intrinsic balance between the protection of individual rights and freedom and the advanced technology. The modern technology may make the lives of people more convenient and easier but sometimes caused severe threat to the privacy of the people when their data's being trade off. The gathering and processing of enormous volumes of personal data has been made by the integration of big data analytics, artificial intelligence, and the Internet. The digital era has enormous potential for innovation, economic expansion, and societal advancement, but it also raises serious concerns about the exploitation and misuse of private data collected by the data fiduciary.

Since we are on the realm of a data-driven era, so we cannot take a chance to compromise with the data privacy as the lives of the people are more entwined with the digital platform. That's why there is need of regulatory framework dealing with the right to privacy in the digital realm. "General Data Protection Regulation (GDPR)" of Europe is the milestone development in the field of personal details and its protection. It was enacted in the year 2018 setting a standard for data protection laws across the world. It establishes the legal framework ensuring the accessibility, confidentiality and securing the transparency, consent and user control. In addition, placed a strong emphasis on individuals' rights to their personal data, requiring enterprises to be open and honest about how they use it, have explicit consent, and put strong security measures in place. The GDPR promoted a culture of accountability by giving people more control over their data and by fining non-compliant businesses severely.

Despite of a global standards set out in the GDPR, threats to cybersecurity are still developing and getting more advanced and focused. Malicious actors continually look for vulnerabilities in digital systems, endangering the privacy of millions of people through ransomware assaults and data breaches. The ethical ramifications of data consumption have also attracted attention. The ethical issues surrounding the acquisition, stockpiling, and use of personal details have taken centre stage in the privacy conversation. It is a difficult but necessary endeavour to strike a balance between innovation and ethics, between data-driven insights and individual rights.

In India, the year 2023 become the milestone for ages when the law on data protection got enacted by the parliament in respect of privacy and data protection. Digital Personal Data Protection Act, 2023 is a step forwarded by the government of India in recognising the importance of securing personal digital data and information. It clearly states that the data

collected can only be used for the purpose it is collected. The Act establishes the Data protection board of India that plays a significant role for compliance of individual personal data protection. The board had immense power to take prompt action against anyone in case of breach of privacy and data protection and imposed penalty up to 250 Cr.

However, challenges and vulnerabilities still exist. The quick rate of technological advancement continuously examine the limits of existing laws. Finding a balance between innovation and privacy protection is still a struggle. Furthermore, the sophistication of cyber-attacks outburst rapidly, underscoring the need for continuous assessment of the implementation of data protection laws.

Education and awareness are recognized as effective measures for defending data privacy. It is crucial to educate people about their rights, the dangers and the consequences of engaging in certain activities online, and how to stay safe while doing so and most important some basic information in respect of what to do and what not to do while providing information online. Additionally, technological solutions also plays a crucial role in preserving data.

Data security and privacy are essential components of a free, safe, and just digital society; they are not just trendy buzzwords. It is a journey not a destination that's why individuals, government agencies, businesses and technology creators must collectively work together to uphold these principles. It is essential for the moral and sustainable development of our digital society, that individuals have control over their personal information, data security, and privacy. A future is where data and privacy are protected, respected. And it will be made possible by ongoing education, lobbying, and responsive policy-making. It necessitates constant attention, flexibility, and contemplation towards morality. However, it is important to understand that the decisions we make today will have repercussions in the future. Thus, we can create a digital world where privacy is not only a right but an unalienable reality by developing a culture of respect for privacy, adopting creative yet moral solutions, and promoting education and awareness.