**Journal of Informatics Education and Research**
**ISSN: 1526-4726**
**Vol 5 Issue 2 (2025)**

# A critical analysis of the data protection act of india (2023): Navigating the socio-legal terrain

**Anusree Bhowmick[1], Dr. Aarushi Batra[2]**

*[1]Research Scholar University of Petroleum and Energy Studies, Uttarakhand, India*
*[2]Assistant Professor, Senior Scale University of Petroleum and Energy Studies, Uttarakhand, India*

**Abstract:**
In the modern era, the exponential rise of data and the rapid expansion of digital technologies have made significant legal frameworks imperative to protect sensitive information and individuals' privacy. In 2023, India got the Digital Data Protection Act 2023, replicating this amplifying context of the digital world. Technology is a dynamic substance that is always evolving and posing new problems. To cope with these evolving problems a thorough analysis of these problems and problems associated with the Digital Data Protection Act 2023 is quintessential in the present socio-legal landscape of India.

In this research, researchers adopted a multi-disciplinary approach leveraging legal, contemporary social, and ethical perspectives. In the course of the critical analysis of the legal framework, researchers manifested the objectives of the legislation, the principle of the act, and the alignment of the global privacy standards. Additionally, this study looked into how this act affected civil rights and how to strike a balance between personal privacy and national security. In addition, researchers offer several recommendations meant to educate legislators, law firms, and the general public.

**Keywords:**
Digital Data Protection Act 2023, Critical analysis, Global privacy standards, Socio-legal context

## Introduction:

Perceiving the necessity to establish the right to privacy more firmly enactment of the Data Protection Act in India was quintessential. Since every sphere of human life including professional and personal life is being digitalized, the security of this orbit should be of the utmost concern. The right to privacy has been recognized as a fundamental right in the KS Puttaswamy case thereafter, the right to data protection has been taken into serious note. When the Supreme Court upheld the right to privacy in the KS Puttaswamy case, J. Chandrachud said this right has both a negative and positive vision. ("Reportable In The Supreme Court India Civil Original Jurisdiction Dr D Y Chandrachud,J" 2014). On the one hand, it restricts what the state can do while also having a positive obligation to ensure the protection of fundamental rights. A data protection bill now assumes the form and shape of preserving informational privacy, which is one of the sub-components of privacy on its own. This act attempts to put Puttaswamy's ruling into effect, but it falls short of doing so.

## A saga of the arrival of the Data Protection Act 2023:

Although the Information Technology Act of 2000 was passed in the year 2000, it did not provide a comprehensive solution for data protection. (Ii *et al.*, 2000)IT (Reasonable Security Practices and Sensitive Personal Data or Information) Rule 2011 was implemented in 2011. It required the body corporate to at least show concern for the handling and security of personal

data. The Supreme Court declared the right to privacy to be a basic right in 2017. (“Reportable In The Supreme Court India Civil Original Jurisdiction Dr D Y Chandrachud,J” 2014). The government had to respect people's privacy when the Supreme Court recognized their right to it. RBI issued a notification in 2018. Customers used to save ecard data while shopping on the internet store. This entity must only store these details in India, per this notification from RBI. In 2019, RBI took a further step and published a fresh notification. It prohibited everyone from saving their card information at all. they could save the card's final four digits(Systems *et al.*, 2020).

The IT (Intermediary Guideline and Digital Media Ethics Code) Rule 2021 came into effect in the year 2021. This guideline required messaging systems like What's App to make it possible to identify the message's first sender. What's App did not support it. As a result, it was contested before the Delhi High Court. The matter is still pending before the Supreme Court. The first draft of a law protecting personal data was created in 2018. The 2019 Personal Data Protection Bill was updated and released. Data Protection Bill 2021 was later updated and released. Surprisingly, the entire law was withdrawn in the name of amendments and revisions. Criminal Identification Act 2022(Delhi, 2022), which replaced the Prisoners Act of 1920, was passed in 2022.('The Identification of Prisoners Act',1920) Therefore, this statute now makes it possible for police officials to gather biometric data including iris, retina, and fingerprint scans. In 2023, the data protection legislation was eventually passed, providing some measure of personal data protection.

**An analysis of definitions and functions of stakeholders**

The Digital Personal Data Protection Bill, 2023 was approved by both the Lower and Upper Houses of Parliament on August 7, 2023, and August 9, 2023, respectively, to protect personal data. It is imperative to first define the word "personal data" before moving on(Government of India, 2023). By section 2 subsection (f) of the Data Protection Act of 2023, "Personal data" refers to any information on a person who can be identified from or in connection with the data. (Government of India, 2023) Even though the distinguishing characteristics in this instance are not extremely clear-cut and distinct, a comparison to the current data protection regulations of other countries may clear and complete the concept. This data may include a person's name, an identifying number, location data, an online identifier, or one or more attributes specific to their physical, physiological, genetic, mental, economic, cultural, or social identity. This is similar to the EU GDPR. In line with the Japan Act on the Protection of Personal Information, this information also includes name, birthdate, and other specifics.(Atsumi & Sakai 2021)

It is also essential to understand the stakeholders and their functions who have been identified by this act. A new organization called a consent manager has been added; it is required to register with the data protection board and has the power to control how data principals who possess and own the data or whose data is being processed provide their consent. The sole authority that can agree to the processing of data is the data principle; however, if the data principal is a minor, child, or someone who is disabled, the legal guardian has that capacity. The person who is taking or collecting the data is designated as the data fiduciary, and he is in charge of deciding why the data is being collected and is accountable for data leakage. Although the purpose is chosen by the data fiduciary, the data is ultimately processed by the data processor, who does the calculations or carries out the act's intended purpose. According to the objective of this law, data principals will be able to manage their consent across several

data fiduciaries with just one or two consent managers using a single dashboard on a smartphone. The consent manager will be linked to the data fiduciary, such as a smartphone application. Of course, all applications that have requested consent may rely on a third-party data processor to carry out the activity. These are the entities that are identified outside of the administration of law by themselves in terms of rights and obligations. Essentially the foundation for data principals has been established by this law. Data is initially gathered from the data principal by the data fiduciary, after which it is processed by the data processor for the same purpose as decided by the data fiduciary and is communicated to the data principal. In the future, if the data principal changes his mind, the consent can be controlled by the consent manager. If consent is not followed or there is a breach of personal data, a complaint can be made to the data protection board for resolution.

**The concept of Data Protection:**

Recently in 2023 Data Protection Act came into force before that the whole data protection regime used to be regulated by the Information Technology Act 2000 in India. That used to deal with all spectrums of technology issues now Data Protection Act 2023 has been enacted to solely deal with digital data and its protection. If section 2 sub-section (h) is explored it states "data" means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means".(Government of India, 2023)That imparts a wide scope of protection and includes data processed by human beings and processed by automated means as well. Being very specific personal data has also been defined under section 2 subsection t "Personal data" means any data about an individual who is identifiable by or about such data". (Government of India, 2023) The identifiable components are not very clear in this section. Apart from that personal data breach, consent manager, data principal, data fiduciary, and data processor. The idea behind the enactment of this act is to make the person who has collected data liable if it is disclosed to a third party without the consent of the concerned party. Third-party information is not defined under the Data Protection Act of 2023 albeit it is defined under the Information Technology Act of 2000. After all data protection means a set of security measures that is used to ensure that data are handled in a way that protects them from unauthorized, unanticipated uses.

**Objective and utility of Data Protection Act 2023:**

The foremost objective of the Data Protection Act 2023 is to secure data and data processing and declare liable the stakeholders who are involved with this processing to the data principal. This act leads a march towards embracing the era of artificial intelligence, cryptocurrency, and blockchain.

Another leading objective and purpose of this act is to sustain transparency, accountability, and fairness. That's why different stakeholders like consent managers, data fiduciaries, and data processors have been recognized in this act. So that fair complaints can be dealt with transparently.

The entire process of protecting these data and processing brings into play other rights that have been recognized by this act. Like the right to erasure, the right to being notified, the right to identify the data fiduciary whom the data is being shared with, receiving a summary of personal data which is being processed, the right to know the purpose of processing of data,

right to nominate. The mission of digital India by the government is now a step forward towards success.

Data Protection Act 2023 is such an act that not only sets liable to data fiduciaries and data processors for their negligence but also the data principal. Which makes every stakeholder liable and imposes high penalties for their wrongful act.

The legislation ensures and secures transborder data transfer i.e. processing data outside India and widens the applicability of this act.

The said act has tried to balance private and public interest incorporating some exemptions in it. However, this leaves room for criticism considering the wideness of the exemption.

Consent is no longer stagnant now. Through consent manager, it can be easily regulated. This act permits to control the consent which was given voluntarily by the data principal. Recognition of the right to erasure gives a new shape to the management of consent.

Assessment of the data is another important objective of this act. Before processing this act ensures the assessment of data on the grounds of sensitivity, and considering the risk of processing multiple times.

**Critical analysis of Data Protection Act 2023**:

In the words of the US Supreme Court

“No right is held more sacred, or is more carefully guarded [...] than the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law”.(Of *et al.*, no date) The goal of the legislation is to grant every person the greatest amount of freedom possible, therefore consent becomes an extremely important factor to take into account. Fundamentally, consent depends on two conditions: first, the possibility to grant particular consent, and second, that there is enough room for decision-making. The "free, specific, informed, unconditional, and clear" consent of the data principle is affirmed by the Data Protection Act. Two sets of individuals from distinct age groups—a child and an adult—make up the data principal. In India, several laws have used various age ranges to classify children. Sec 2 subsection I of this act considers below 18 years of age in the category of child.

**Wide exemption to government:**

Consent is a long-standing custom that fundamentally develops from patient-provider consent. How patients who are undergoing any kind of medical operation are informed of the hazards and the precise reasons why they are giving their agreement to have their body operated on. The person who is being put on notice will be informed of the procedure's purpose before having the option to be examined. The notice and consent provisions in this statute are similar. However, other exclusions have been made available, therefore negating the need to obtain consent. It grants both the public and private sectors numerous exclusions. The phrase "certain legitimate uses" is now listed under section 7 of the Data Protection Act of 2023, where it was previously referred to as "deemed consent" in the previous bill and was vehemently opposed. (Government of India, 2023)

**Epidemic allows the government to collect data without the consent of the concerned person:**

No permission is required when a disease outbreak or epidemic occurs to collect data during a pandemic of COVID-19. Several data breach events that occurred in India during COVID-19 demonstrate that the government has very little control over the operation of large-scale databases that were used to gather and register data and for which the government had promised to provide the safest environment. Data breaches have occurred before with Aadhar and numerous other private-sector databases, therefore this is not the first instance of them. The Telegram bot during the COVID-19 epidemic displayed the name of the individual receiving the vaccination, the government ID they used, and the location of the immunization. It has been reported that a government server leak has made the names, mobile numbers, addresses, and COVID test results of thousands of Indian citizens publicly available online.

The compromised data has been listed for sale on the Raid Forums website, where a hacker claims to have access to the private data of over 20,000 people. Each person's name, age, gender, cell phone number, address, date, and COVID-19 report conclusion are all posted on Raid Forums. Government officials have denied their callousness and said that reports of data leaks are malicious. After analyzing the scenario, it can be said that the information gathered from the general public for their safety during a pandemic has a significant impact on their personal lives and liberties.(‘united-states-leads-seizure-one-world-s-largest-hacker-forums-and-arrests-administrator @ www.justice.gov’, no date) The history reveals a grave repercussion of wilfully disclosing personal information to the government, which jeopardizes personal life. The section 7(g) exemption broadens the scope of such data breaches by enabling government data collection even in the absence of data principal permission. (Government of India, 2023)

**Arbitrary data Collection of employees by employer:**

Any employer may gather an employee's personal information without the employee's knowledge under section 7(i) of the Data Protection Act 2023, and no notice of the collection of the employee's personal information is required. The Right to Information Act's section 8(1)(j) states that certain information is exempt from disclosure because it "relates to personal information the disclosure of which has no relationship to any public activity or interest." The referenced section of the Data Protection Act of 2023 defines the purpose of data collection as "safeguarding the employer from loss and liability." This is a very broad purpose, and the fact that the employer has sole discretionary power of loss and liability expands the potential for employee privacy violations. Employers are permitted to request any personal information from employees by this provision to protect themselves from loss and liability. The breach of sensitive information, including passbooks, names, addresses, contact information, and PAN numbers, involving 12000 SBI employees in India should be taken extremely seriously when it comes to employee privacy and data protection. 260GB of sensitive personal information of employees, including name, phone number, bank information, parents' names, date of birth, salary, payslip, tax information, and even photocopies of personal documents like a driver's license and voter ID, were exposed in a data breach reported by cyber news on January 18, 2023. which affected 2,000 employees and nearly 9,000,000 job applicants.(‘telegram-channels-leak-data-of-12-thousand-sbi-employees-ignored-some-red-flag-2405024-2023-07-11 @ www.indiatoday.in’, no date)

**Imprecise Data Protection Impact Assessment Procedure:**

Sec. 10(2)(c)(i) guarantees periodic data protection impact assessments, but it doesn't fully explain the purpose or process of these assessments, leaving many questions unresolved. If General Data Protection Regulation Article 35 is applied, the concept of recurring data protection impact assessments may develop.(Article, 2006)

.

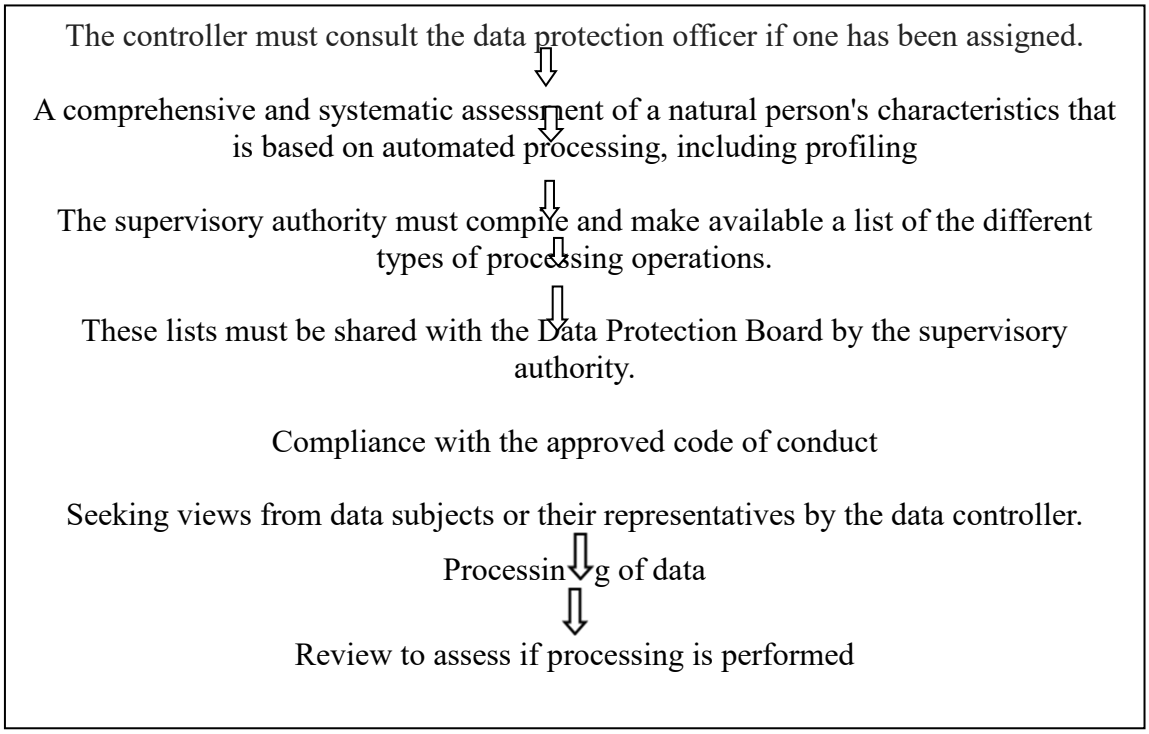



**Table1: Data Protection Impact Assessment Procedure**

**Minor disobedience of duties by the data principal might disqualify him from enjoying his rights:**

Data principals, who are intended to be safeguarded by law, are not subject to obligations in terms of penalties for violations. It is not only a protection of the law, but it also gives the data principle a positive obligation to abide by the rules of the aforementioned act as a regular person. When the data principle exercises his rights, such as the consent to notification or the right to correction for access to data, disobedience with even a minor provision of the law disentitles him from the protection of the law. Furthermore, section B's prohibition on impersonation indicates that the data principal is not permitted to act as a proxy for someone who might be incapacitated. When a person is elderly and digitally illiterate alone, their level of incapacity may occasionally extend to them. That could be evidence of bad faith to assume the individual is impersonating someone else.

**Duty of data disclosure on data principal:**

Section 15 subsection C of the Data Protection Act 2023 enunciates that the data principal has a duty "to ensure not to suppress any material information while providing her data for any document, unique identifier, proof of identity or proof of address issued by the State or any of its instrumentalities" which implies that a person must disclose all relevant information when supplying personal information for any document that requires a unique identifier, identification, address, or state evidence.(Government of India, 2023) This means that even if a private company requests a data principal's contact information and other sensitive personal information, even if the data principal does not want to share it with the designated person,

failure to comply with any duty could result in the loss of enjoyment of the entire act. The responsibility for digitization and promoting Digi Bharat is typically placed on tech companies, and this law permits tech companies to approach data principals for personal information. People frequently give erroneous information because their levels of sensitivity vary.(‘Digital India A programme to transform India into a digitally empowered society and knowledge economy What is Digital India ?’, no date) For instance, young women with careers may choose not to disclose their full addresses or personal identifiers, which increases the possibility of stalking. However, each of these obligations is very clear in comparison to other data protection laws around the world, and if any obligation listed in Schedule 5 of the Data Protection Act of 2023 is broken, a fine of 10,000 rupees may be imposed as a result, according to Section 15 of the law. The statute was written so that every violation subjected the data principal to punishment.

**Prevention of frivolous grievances leads to a high risk of paying the fine by data principles:**

The duties under clause 15(d) also include a clause requiring the data principal "to ensure not to register a false or frivolous grievance or complaint with a Data Fiduciary or the Board," which implies that the data principal is not permitted to file a false frivolous complaint with the data protection board.(Government of India, 2023) Not everyone has the investigative skills necessary to determine whether the problem they are dealing with is real. Aged people who lack technical proficiency and awareness may be victimized by this statute. Due to the high risk of receiving a fine, people will be reluctant to file complaints.

**The intervention of the Central government of the Data Protection Board**

Data Protection Act 2023 does not have a regulatory body per se. This act created the Data Protection Board, a regulatory entity that is essentially a ruse. The central government now holds monopoly control over the entire operation of this board. Every member of the board, including the chairperson, shall be selected by the central government, by Section 19 of the statute. Even the central government has the authority to remove these board members.

The chairperson and other members shall hold office for a term of two years and shall be eligible for reappointment, according to Section 20 Subsection 2 of this statute. (Government of India, 2023)It suggests that the central government has been granted the discretionary power of reappointment. The central government has the power to decide whether the board will be established and continue to function. Members are expected to be nominated for terms of two years.

Under section 18 of the said act a very ambiguous norm is established by the central government's notification, which leads to the data protection board being pointed out.(Government of India, 2023) Under this statute, the central government may suo moto protest to the data protection board and request information from it as well. The data protection board must be a self-governing organization. It is a particular type of judicial body that is expected to operate impartially and independently. The central government's interference not only ruins the ethics of the division of powers but also disturbs the regular flow of business. If other nations' data protection laws, such as the General Data Protection Regulation and the French Data Protection Act, are followed, the data protection board is seen as an autonomous body that is free to act and make decisions without outside interference.(Franch National Assembly and the Senate, 1978)

The federal government has extensive influence over the execution of this law, both in terms of notice and in terms of complaints. Pure conflict of interest raises serious concerns about transparency.

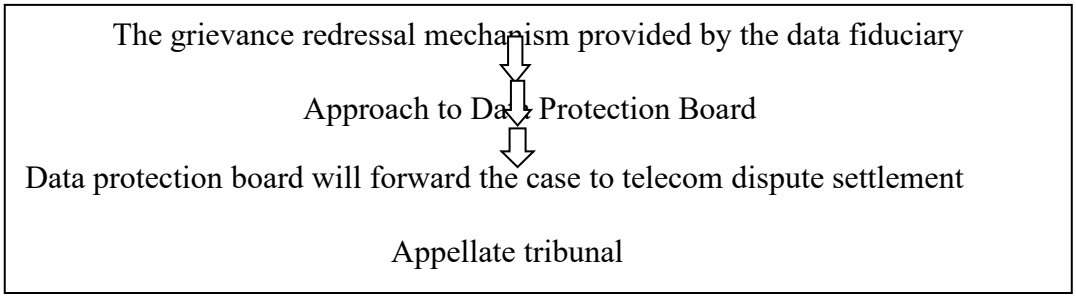
**Balance of private and public interest:**
The right-to-information legislation, which has been a game-changer in bringing accountability together, basically has a body of exemptions where information can be requested from public authorities. The well-balanced right-to-information law includes an exemption for the right to privacy under section 8(1)(j). It does not just state that any private information is exempt and cannot be disclosed in response to a right-to-information request. Additionally, it states that the refusal of the information must be reasonable and serve the public interest, indicating that the right-to-information legislation takes privacy into account. However, when a statute is properly understood, the public interest is given more weight. Therefore, they must be balanced so that a better level of value is offered.

**Right to erasure and right to be forgotten:**
Section 12 subsection 1 of Data Protection Act 2023 elucidates "A Data Principal shall have the right to the rectification, completion, updating, and erasure of her data for the processing of which she has previously given consent, including consent as referred to in clause (a) of section 7, under any requirement or procedure under any law for the time being in force". (Government of India, 2023)This implies that a data principle has the power to request the data fiduciaries to delete data that he contributed with his consent for a specific purpose. However, there are numerous instances in India where the media eavesdrops and collects information without authorization, which is then visible to everyone through search engines and databases. If EU GDPR is examined, art. 17's protection of data obtained with and without consent has a broad scope. Which encompasses the right to be forgotten and the right to erasure. Google Spain SL's definition of the right to be forgotten court. According to Vs Agencia Espanola de Proteccion de Datos, a national court's intervention is necessary to determine if the current connection from the search engine should be removed or not.(‘Guía de Protección de Datos por Defecto’, 2020)There is no specific language on judicial involvement in the Data Protection Act of 2023, and the Data Protection Board, which is theoretically under the control of the federal government, now has sole decision-making authority.

**Exemption to startup companies:**
Section 17 (3) of the current data protection legislation exempts start-up businesses from complying with Section 5, Subsections (3) and (7) of Section 8 and Sections 10 and 11. The term “startup” includes private limited corporations, partnership firms, and limited liability partnerships incorporated in India.(Government of India, 2023) Therefore, start-up businesses are exempt from notifying the data principal before processing data. If the data processing loses its accuracy and transparency, the data fiduciary is not responsible to the data principal. If the data is processed by a start-up company, no data evaluation regarding the sensitivity of the data and processing risk will be performed. This is a broad exception granted to start-up companies that could result in widespread data theft.

**Complicated Tiered mechanism**.

People who feel they have been wronged by the law must first go through the data fiduciary's grievance procedure. They will be able to contact the Data Protection Board after they have exhausted this option. Telecom dispute resolution and appellate tribunal will hear appeals from the Data Protection Board. The system is made more difficult and time-consuming by this tiered method. Data spreads so quickly in the digital age that using this approach won't help.




**Conflict between sec 43A of the IT Act 2000 and 44(2) of data protection act 2023**:
Section 43a of the IT Act 2000 imposes an obligation on corporates to award damages to the affected persons in case of negligent handling of their sensitive data. Section 44(2) of the Data Protection Act 2023 aims to exclude the application of sec 43a thereby rendering an individual who has suffered breach of their data without any relief. Now if a data breach occurs due to the negligence of a body corporate which includes any company or government that holds the data is free from any liability that was secured by sec 43a of the Information Technology Act 2000 and has been taken away by the Data Protection Act 2023. Now government is free to misappropriate data that is being collected about Aadhar and other identity credentials.(Ii *et al.*, 2000)

Mr. Bhaseer, an Aadhaar card bearer, petitioned the Delhi High Court in 2018 about how the voluntary Aadhaar scheme had been transformed into a mandatory compulsion. Aadhar link is now required for all activities, including banking, filing tax returns, and cell phone subscriptions. The petitioner further claims that respondents breach the fundamental privacy rights of the petitioner and the general public by carelessly jeopardizing the security of Aadhaar data and requests reimbursement under the Information Technology Act 2000 Section 43A(‘89a3270cd97a4953afdb29678f959a9ab7f29e77 @ www.livelaw.in’, no date). Now that Section 44(2) of the Data Protection Act of 2023 has been incorporated, the government and businesses that hold data are released from all liabilities, and the data principal is no longer eligible to claim compensation.(Government of India, 2023) Now, data can be unlawfully acquired by unauthorized third parties who are always free to utilize it against the owner's interests.

**Success towards the accomplishment of objectives:**
Though the effectiveness of this act will be revealed with time the present framework comes up with a lot of flaws that might stand as a hurdle in the way of success. Nevertheless, primarily the objective of this act was to maintain transparency, accountability, and fairness but the provisions that have been incorporated in this act speak different tales. Providing wide exemptions to the government, and putting unnecessary obligations on data principals do not reflect enough transparency in it. To some extent, it is unable to maintain a parity between public and private interests. It also creates conflict with the Information Technology Act 2000

though initially, the purpose of this act was not to contradict any existing laws about this topic.

The objective of the act is to grant a speedy remedy. Implementation of filing a complaint and receiving remedies seems very time-consuming when the lengthy procedure of filing a complaint is taken into consideration. Which might create problems and hard to understand the people belonging to the old age group.

Putting arbitrary control over the data protection board by the central government reflects monopolization of power of government where ethics of separation of power also falls apart.

**The alignment of the global privacy standards:**

For significant Commercial growth industries tend to resort to AI development. The Indian government has taken several initiatives to make a robust AI infrastructure. IUSSTF inaugurated US-India Artificial Intelligence on March 18th, 2023, intending to create a robust forum for idea sharing, investigating R&D potential, and bolstering the prospects for collaboration between the two nations. Global privacy standards ensure ethical data processing by Art 13,14 and 22 and promote an automated decision-making process. It is obscure in the Digital Data Protection Act 2023 whether India has the same desire to enact governing frameworks on AI development.

A globally acknowledged right is the one to have a response within a reasonable amount of time. Although India has established a body to which complaints may be submitted, no deadline for filing complaints has been mentioned, undermining the intention and goals of its establishment.

Globally GDPR compliance audit is recognized and prevalent. A complaint audit is a checklist and a systematic assessment of whether the provisions are being complied with by people. That meets the main purpose of the enactment of any legal framework. Digital Data Protection Act 2023 applies even to the processing of personal data outside of India if the data transaction is connected to any territory of India. When the ambit of the application of this legislation is so wide a mandate to conduct an audit is required.

The mode of contacting to data protection officer is not clear through the present Data Protection Act of India. Nor any office has been determined. Globally Data are being transacted with India. An agent should be appointed to ease the process of filing a complaint.

**Suggestion and Conclusion:**

To keep the essence of this act certain changes are quintessential to incorporate. Initially, the purpose of enactment of this act was to sustain fairness but accumulation of power in the hand of the central government loses its purpose. Eventually, it fails to achieve the goal. Exemption of sovereignty and public order is a normal phenomenon, but exempting in every flexion makes the term “consent” unworthy.

This allows the government to collect data during an “epidemic, outbreak of disease, or any other threat to public health” without the consent of the data principal. Sensitive data like the data of employees has been set free to collect by employers for the sake of trade secrets and any service or benefit. Removal of these two exemptions is very important to maintain parity.

The imposition of huge fines on data principals on trivial issues causes fear of filing complaints in the minds of data principals. A 10000 Rs. fine for a frivolous complaint is huge, a reduction of this amount is recommended

Easing the complaint filing procedure is very important. Already enough stakeholders are there to take care of the authenticity of the complaint. Unnecessary stretching of the procedure leads to delays in getting remedies and complications.

The Data Protection Board should be autonomous since it will work as a quasi-judicial body. Continuous monitoring and sole control of the government vitiates the purpose of forming this body.

Sec 12 of the Data Protection Act should deal with any kind of personal data. It should not discriminate based on consent. It solely deals with and protects data that are collected with the due consent of the data principal. In India, a lot of data are collected without the consent of the data principal and remains deprived of the protection of sec 12 which authorizes the data principal to erase data which they voluntarily gave to the data fiduciary.

"Startup" company is itself a very wide term which includes both private and public companies. Giving them deliverance from obtaining consent from data principals to collect data is a real threat. This section should be narrowed down specifying which sort of companies are falling within this ambit.

The omission of sec 43(2) of information is a real menace.
Data Protection Act 2023 of India could have been remarkable legislation if these flaws could have been removed. Bringing balance to the power of stakeholders and prioritizing the interest of the data principal should have been the utmost matter of consideration. This legislation has failed to achieve that. Accumulation of too much power in the hands of the government not only degrades the value of this act but the ethics of the democracy somehow gets vitiated. Now India is standing in a position despite having the Data Protection Act to protect personal data this cannot be considered to be fully effective and fruitful.

**References:**

1. '89a3270cd97a4953afdb29678f959a9ab7f29e77 @ www.livelaw.in' (no date). Available at: https://www.livelaw.in/delhi-hc-issues-notice-on-prof-shamnad-basheers-petition-seeking-exemplary-damages-for-aadhaar-data-leak-read-petition/?infinitescroll=1.
2. Article, G.P. (2006) 'Act on the Protection of Personal Information ( Act No . 57 of'.
3. ATSUMI & SAKAI (2021) 'A Guide to Data Protection in Japan', (September), pp. 1–26. Available at: https://www.aplaw.jp/data-protection-202009.pdf.
4. Delhi, N.E.W. (2022) 'xxxGIDExxx vlk / kkj . k bl Hkkx esa fHkUu i ` " B la [; k nh tkrh gS ftlls fd ; g vyx ladyu ds : i esa j [ kk tk ldsA MINISTRY OF LAW AND JUSTICE ( Legislative Department ) THE CRIMINAL PROCEDURE ( IDENTIFICATION ) ACT , 2022 An Act to authorise for taki', 235184(Dl).
5. 'Digital India A programme to transform India into a digitally empowered society and knowledge economy What is Digital India ?' (no date).
6. Franch National Assembly and the Senate (1978) 'ACT 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties'.
7. Government of India (2023) 'Digital Personal Data Protection Act 2023', *The Gazette of*

*India* [Preprint], (Dl). Available at: https://www.meity.gov.in/writereaddata/files/Digital Personal Data Protection Act 2023.pdf.

8. 'Guía de Protección de Datos por Defecto' (2020).
9. Ii, C. *et al.* (2000) 'THE INFORMATION TECHNOLOGY ACT , 2000', pp. 1–36.
10. Of, B. *et al.* (no date) 'S upreme Court of the United States', 20001(18).
11. Systems, S. *et al.* (2020) 'Department of Payment and Settlement Systems, Central Office, 14', 2020(1810).
12. 'telegram-channels-leak-data-of-12-thousand-sbi-employees-ignored-some-red-flag-2405024-2023-07-11 @ www.indiatoday.in' (no date). Available at: https://www.indiatoday.in/india/story/telegram-channels-leak-data-of-12-thousand-sbi-employees-ignored-some-red-flag-2405024-2023-07-11.
13. 'THE IDENTIFICATION OF PRISONERS ACT , 1920 THE IDENTIFICATION OF PRISONERS ACT , 1920' (1920), pp. 1–5.
14. 'united-states-leads-seizure-one-world-s-largest-hacker-forums-and-arrests-administrator @ www.justice.gov' (no date). Available at: https://www.justice.gov/opa/pr/united-states-leads-seizure-one-world-s-largest-hacker-forums-and-arrests-administrator.
15. Burman, Anirudh. "Understanding India's New Data Protection Law." Carnegie India, October 3, 2023. https://carnegieindia.org/2023/10/03/understanding-india-s-new-data-protection-law-pub-90624.