



JOURNAL OF DIGITAL LAW, PRIVACY & CYBER GOVERNANCE

ISSN No. _____

Volume 1 | Issue 1

2026

© 2026 *Journal of Digital Law, Privacy & Cyber Governance*

Follow this and additional works at: <https://www.quillifypub.com/>

This article is brought to you for free and open access by the Journal of Digital Law, Privacy & Cyber Governance. It has been accepted for inclusion in the Journal of Digital Law, Privacy & Cyber Governance after due review.

In case of any suggestions or complaints, kindly contact info@quillifypub.com.

To submit your Manuscript for Publication in the Journal of Digital Law, Privacy & Cyber Governance, kindly email your Manuscript to <https://www.quillifypub.com/submit>.

Shining a Light on the DPDP Act: Battling Dark Patterns and Amplifying Transparency

Chirag Rastogi

Advocate

Anirudh Alex Victor, Advocate, Email: anirudhvictor999@gmail.com Ph no. [contact withheld])

Abstract

The interplay between dark patterns, privacy protection, and privacy in the context of India's evolving digital ecosystem served as the impetus for the founding principle of the "Right to be left alone." The paper underscores pivotal roles of transparency and privacy in shaping digital experience of 21st century by acknowledging India's stands as the second-largest internet market. DPDP Act has been introduced and certain key provisions such as Data principal, significance of clear consent and roles of data fiduciaries and processors standards has been emphasized with emergence of dark patterns and their potential threat in coercing users into unintended data disclosures.

DPDP Act has been critically analysed and its impact on user privacy dissecting its provisions and scrutinizing potential loopholes. It explains attentively and its role in combating deceptive design practices known as dark patterns by establishing link between data protection and user experience contributing to ongoing discussions on ethical design and responsible data handling. It highlights potential challenges in implementation, especially concerning expansive authority granted to central government and amendments affecting Right to Information Act.

It underscores necessity of a legal definition of privacy, advocates for more explicit provisions related to non-personal data and calls for additional legislation addressing dark patterns. It critiques structural issues within Digital Protection Board and asserts need for a nuanced approach in balancing innovation and privacy protection. As digital landscape evolves, it contributes to ongoing dialogue on ethical design, responsible data handling, delicate balance between innovation and privacy protection in the digital age.

Keywords: Digital, Data Protection, DPDP Act, Dark pattern, Privacy,

Introduction

Legal scholars Samuel D. Warren and Louis Brandeis influenced and given then the concept that individual possess the inherent "*Right to be left alone*" as a fundamental facet of privacy in an article "*Right to Privacy*."¹ The founder of Social media networking site VK and creator of telegram messenger, Pavel Durov, once shared his perspective, "*Privacy is not for sale, and human rights should not be compromised out of fear or greed.*"

¹ Samuel D. Warren & Louis D. Brandeis, Right to Privacy, 4 Harvard Law Review.193, 195 (1890).

In India there are 700 million users actively engaged on internet² and established as the second-largest internet market globally³ that's the reason transparency and privacy both plays pivotal roles in the digital world of 21st century in shaping our overall digital experiences and to fulfil this objective, India's legal system consistently strives to make progress.

As we all know that innovation and invention contribute to society's progress but same forces also fuel the criminals and with the rise in internet usage, dark patterns have emerged, many individuals, organizations or entities are actively engaged in deliberative tactics aimed at coercing users into disclosing information contrary to their intentions and personal interests.⁴

In this research paper we are going to discuss about the recently enacted data protection law, examine its potential impact on safeguarding user privacy. Additionally, we scrutinize the use of dark patterns in digital world by exploring the intersection of data protection and user experience, we aim to contribute on the ongoing discourse on ethical design and responsible data handling further we are going to talk about criticism of this digital act.

Research Methodology

This paper employs a descriptive approach, by utilizing qualitative research methods such as literature review, document analysis, and case studies to conduct a comprehensive exploration of the subject matter.

1. Extensive literature review: A thorough examination of scholarly articles, legal documents, publications, reports, and online resources concerning the Data protection in India.
2. Case Studies: In-depth exploration of specific legal cases, including notable disputes regarding the privacy in K.S. Puttaswamy and misleading consumers in LinkedIn case.
3. Ethical Considerations: Throughout the research process, ethical principles will be upheld, ensuring confidentiality, respect for participants, and transparent reporting in all stages of data collection, analysis, and dissemination.

Review of Literature

The literature on Digital protection framework in India sheds light on several critical issues, Chief among these concerns are the privacy of individuals, dark patterns and the limited legal safeguards available. Scholars argue that the Dark pattern misleads consumers or citizens which ends in going contrary to their intentions. Moreover, the lack of how to use Internet knowledge harms the citizens and they get into the trap of dark pattern, legal scholars emphasize the imperative for legislative reforms designed to rectify these deficiencies, advocating for the establishment of a robust framework that ensures the digital protection for citizens in the evolving landscape. This review contextualizes the Digital Personal Data Protection Act, 2023, within the broader discourse on privacy laws and digital information management.

² Economic Diplomacy Division, <https://indbiz.gov.in/india-had-over-700-mn-active-internet-users-by-dec-22-report> (last visited Nov. 13 2023).

³ Invest India, <https://www.investindia.gov.in/sector/retail-e-commerce> (last visited Nov. 13 2023).

⁴ Christoph Bosch, Benjamin Erb & Frank Kargl, Tales from the Dark Side: Privacy Dark Strategies and Privacy 2016 Dark Patterns, *Proceedings on Privacy Enhancing Technologies* 237, 242-249 (2016).

Data protection

Right to Privacy is the part of the fundamental right 'Right to Life' enshrined under Article 21 of the Indian Constitution.⁵ Hence, Data protection is not just necessary it is paramount in today's digital world, as the growth advancement in technology, coupled with the widespread digitization of personal and organizational information, have underscored the critical need for robust data protection measures and to fulfil the objectives of data protection and maintain balance between transparency and privacy India has enacted *Digital Personal Data Protection Act, 2023* which aims to protect the data of citizens ensuring their privacy and holding entities accountable for responsible data management.

Key provisions of the act-

1) Data Principal: The person whose data belongs to is known as the data principal, the person to whom the data pertains or related to. For example. A signs up for social networking site. In this scenario, A is the data principal because the personal data, such as his name, address etc. is directly related to him. [Sec. 2(j)]

2) Consent: Consent is defined in section 13 of Indian Contract act 1872, when two persons agree upon same thing in same sense that is "*Consensus ad idem*" and Section 4 of the DPDP Act, 2023 says that processing of personal data is permissible only after taking consent to whom the data belongs (data principal) and for explicitly stated purposes. In simple terms Data fiduciaries has to take consent from data principal and tell the specific purpose of demanding the data. The consent must be freely given means it is not caused by coercion, undue influence, fraud, misrepresentation or mistake,⁶ specific, well-informed, without conditions, and expressed unambiguously through a clear affirmative action as per section 6 of the DPDP Act, 2023.

3) Data Fiduciary: Any person or group of persons, who collectively or independently decides the purpose and methods of data processing. In simpler terms, data fiduciary is someone who has control over why and how personal information is managed. For example, ABC Mart collects personal information from its customers data process orders and provide personalized services here, ABC Mart is Data fiduciary. [Sec. 2(i)]

4) Data Processor: Any individual or entity that manages personal data on behalf of data fiduciary are known as Data Processor, they process data as directed by the entity that is responsible for the data that is data fiduciary. For example XYZ Corporation decides to start cloud storage service to manage and store the data of their employees, Cloud Vault possess the data on behalf of XYZ. In this case XYZ is data fiduciary, employees are data principal and Cloud Vault is data processor. [Sec. 2(k)]

Historical Context of Data Protection Legislation

The evolution of data protection laws reflects society's response to the challenges posed by the digital age. It traces back to landmark initiatives such as the Fair Credit Reporting Act (FCRA) in the 1970s, which aimed to regulate the collection and sharing of consumer credit data in the United States. The European Union later introduced the Data Protection Directive of 1995, establishing key guidelines for personal data processing. The transformative General Data Protection Regulation (GDPR) of 2018, inspired by the Directive, imposed stringent obligations on companies handling personal data globally. Concurrently, the US enacted the Health

⁵ K.S. Puttaswamy v. Union of India, AIR 2017 SC 4161.

⁶ The Indian Contract Act, 1872, § 14, No. 9, Acts of parliament, 1872 (India).

Insurance Portability and Accountability Act (HIPAA) in 1996, ensuring security for medical data.

High-profile data breaches, like the 2017 Equifax hack and the 2018 Cambridge Analytica scandal, underscored the need for stronger data protection measures. This historical context sets the stage for the Digital Personal Data Protection Act of 2023, representing a deliberate effort to enhance personal data protection amid unprecedented digital connectivity and information exchange.

Dark Pattern

In 2010, “Dark Pattern” a new term introduced by Harry Brignull who was London based UX designer, describing the deceptive tactics employed in websites and applications. These tactics manipulate users into unintended actions, such as making purchases or signing up for services without their intention,⁷ Dark Patterns are also known as deceptive designs.⁸ The essence of consent is undermined by dark patterns, deceiving users into “agreeing” or “accepting” the terms and conditions that they would not accept or significantly modify their preferences, this makes consent concept irrelevant.⁹

Dark patterns are presented here for an extensive period, we can say beyond online interfaces. As an illustration, certain credit card statements may highlight a 0% balance transfer, yet the fine print may not clearly convey that the percentage will escalate significantly unless the user commits to a lengthy agreement.

In past, there was classic pop-up ads were notorious ads were notorious for misleading users with claims of winning random sweepstakes, inundating them with spam. In the contemporary web landscape, Dark Patterns have evolved into more sophisticated and deceptive forms. Brownlee (2015) provides a notable example involving LinkedIn, where automated follow-up email reminders were sent on behalf of new users to contacts obtained from their webmail accounts. These emails were meticulously crafted to appear as if they originated directly from the user.

There was a time when LinkedIn was to be notorious for inundating inboxes with numerous follow-up emails through user contacts, ostensibly to "expand professional networks." Escaping from this pattern proved challenging. Recognizing this deceptive practice, a class-action lawsuit was filed against LinkedIn in San Jose's US District Court (Perkin v. LinkedIn, 2014)¹⁰, with the primary issue being spam.

This legal action resulted in LinkedIn facing a class-action lawsuit and a penalty of \$13 million. It not only held LinkedIn accountable but also sent a cautionary message to other companies employing similar tactics and dark UX patterns to artificially boost their product growth. This serves as a reminder of the legal consequences and ethical implications associated with deceptive practices in user experience design.

Types of Dark Pattern

Brignull further talks about the 10 types of dark patterns which are as follows:

⁷ Deceptive pattern, <https://www.deceptive.design> (last visited on Nov. 14 2023).

⁸ Narayanan A, Mathur A, Chetty M & Kshirsagar M, Dark patterns: past, present, and future: the evolution of tricky user interfaces. 18 Queue. 67-92, (2020).

⁹ Ari Ezra Waldman, 31 Cognitive biases, dark patterns, and the ‘privacy paradox’, 3 Current Opinion in psychology. 105, 106-109 (2020).

¹⁰ Perkins v. LinkedIn Corporation, 53 F. Supp. 3d 1222 (2014).

1) Bair and Switch- This phenomenon occurs when intention of user is something and result is unexpected or unforeseen consequence. For example, in windows 10 upgrade, clicking X at the top right corner of an upgrade pop-up closes the window without additional repercussions.

2) Disguised Ads- This strategy is employed to create an blurry moment or illusion, It is a deceptive design pattern wherein advertisements are intentionally camouflaged within the page to mimic regular content or navigation elements, these ads seamlessly blend into the natural flow of the webpage, making users more likely to click on them inadvertently.

3) Forced Continuity- It is a prevalent dark pattern found on various subscription based websites which at first offers free trials, once the trials conclude users are automatically charged without any opt-out options, reminder, or straight forward cancellation process.

4) Friend Spam- When a product requests the user's mail or social media permissions with the promise of a beneficial outcome, such as helping them find friends but the product subsequently abuses these permissions by sending spam messages to all of the user's contacts, falsely appearing as if the messages were initiated by the user.

5) Hidden Costs- The concept of navigating through numerous steps only to encounter unforeseen charges at the final step in the checkout process, such as unexpected delivery charges or other taxes, is characterized as the phenomenon of 'concealed expenses.'

6) Misdirection- This design strategy aims to strategically guide user's attention, leading them to overlook certain elements or actions while emphasizing or highlighting others. It occurs when the focus of the user is intentionally directed to a particular area, diverting their attention away from another activity.

7) Price Comparison Prevention- This strategy is used create obstacles for the user when he attempts to compare the price, the objective is to impede the user's ability to make an informed decision by introducing complexities or hindrances.

8) Price Zuckering- This deceptive strategy is related to privacy setting and information sharing on online platforms, It is derived from the name of Mark Zuckerberg, the co-founder of facebook, It involves designing user interface in such a way that encourages or tricks users to disclose their personal information more than they wants to.

9) Roach Motel- This dark pattern is used to create a user interface that facilitates effortless entry into a particular situation or commitment, only to complicate and impede the user's ability to extricate themselves from that situation, this dark pattern is a frequently encountered and universally relatable design strategy.

10) Tricky Questions- This strategy involves the presentation of a question that, when quickly glanced at, appears to be asking one thing but, by looking closely, reveals a different intent.

Link between Dark Pattern and Digital protection Act

In this digital age where the data is recognized as valuable currency, the DPDP Act, 2023 stands as pivotal regulatory framework, aiming to safeguard user privacy, this framework for ethical data handling but also serves as a formidable defence against the pervasive threat of dark patterns let us understand how-

1) Clear Consent Standards:

- obtaining "consent" is mandatory, all entities must seek approval from the "Data Principal" before processing the data

- Section 6 sets clear standards for obtaining user consent, emphasizing that it must be free, specific, informed, unconditional, and unambiguous.
- This clarity directly addresses the deceptive nature of dark patterns that often rely on confusing or ambiguous language to manipulate users.

2) Affirmative Action Requirement:

- The requirement for a clear affirmative action ensures that users actively and knowingly agree to the processing of their personal data.
- Dark patterns often exploit passive or unclear consent mechanisms, and the affirmative action requirement serves as a barrier against such manipulative practices.

3) Transparency and Informed Decisions:

- By mandating informed consent, the DPDP Act ensures that users have access to necessary information about how their data will be used.
- This transparency is a direct countermeasure to dark patterns, which thrive on misleading users about the consequences of their actions.

4) Limiting Data Collection:

- Section 6 stipulates that consent should be limited to the personal data necessary for the specified purpose.
- Dark patterns may attempt to collect more data than necessary, and this limitation acts as a safeguard against overreaching data collection practices.

5) Legal Consequences for Violations:

- The DPDP Act likely includes penalties for non-compliance, creating a deterrent for entities engaging in dark pattern practices.
- Knowing the legal consequences reinforces the importance of obtaining consent in accordance with the act's provisions.

In simple words, DPDP Act, 2023 directly addresses the tactics employed by dark patterns by establishing clear standards for Obtaining user consent, promoting transparency, and limiting data collection. This, contributes to the overall effectiveness of the act in combatting deceptive practices in this digital age.

Implications on Businesses & Organisations

The Digital Personal Data Protection Act, of 2023, has a dramatic impact on a range of stakeholders, including corporations, government agencies, and non-profit organizations, and it fundamentally alters the data management landscape.

Implication on Businesses-

1. **Enhanced Data Governance Requirements-** The Act requires enterprises to have a strong data governance system. This includes procedures to guarantee adherence to the Act's requirements as well as explicit policies on data collection, processing, and storage. To protect personal data, businesses will need to put organisational and technical safeguards in place.
2. **Increased Accountability and Transparency-** Nowadays, companies must adhere to stricter guidelines for transparency and accountability while processing data. They have to give

people easily readable privacy notices that explain why data is being gathered and how it will be used.

3. **Investment in Compliance Measures-** Businesses will probably need to set aside funds for compliance initiatives, which may include hiring new employees, updating outdated technology, and consulting attorneys. This could involve a large financial outlay, especially for smaller companies.

Impact on Government Agencies-

1. **Protection of sensitive information-** Like companies, nonprofits handle personal data frequently, particularly in the social services and healthcare sectors. The Act's provisions guarantee that these organisations must maintain data protection standards that are comparable to those of other entities.

2. **Resource allocation for Compliance-** Like companies, non-profits handle personal data frequently, particularly in the social services and healthcare sectors. The Act's provisions guarantee that these organisations must maintain data protection standards that are comparable to those of other entities.

Compliance Challenges & Opportunities for Businesses-

1. **Navigating Complexities of Data Handling-** Companies may find it difficult to manage the complexities of data handling, especially if they operate in several jurisdictions with various data protection laws. Maintaining compliance in a variety of operational domains could be difficult.

2. **Technological adaptations-** Technical difficulties may arise in modifying current systems and procedures to comply with the Act's requirements. This can require spending money on personnel training, data protection protocols, and new technology.

3. **Competitive Advantage through Data Ethics-** Businesses that prioritise data ethics and privacy above and beyond the requirements of the Act may find themselves at a competitive advantage. Establishing a commitment to responsible data processing can improve stakeholder and customer trust.

In summary, a paradigm shift in the management and protection of personal data is brought about by the Digital Personal Data Protection Act, 2023. Businesses and organisations face difficulties with compliance, but there are also chances for better data governance and moral behaviour. Stakeholders must successfully navigate these complexity if they are to grow and adjust to the changing data protection landscape.

Ensuring Compliance

For enterprises to protect personal information and respect individuals' rights, compliance with the Digital Personal Data Protection Act, 2023, is essential. Achieving and sustaining compliance requires the application of suitable tools and methods, best practices, and practical guidance.

1. **Conduct a Comprehensive Data Audit-**

Start by thoroughly auditing every organisation's data management procedure. Determine what information is gathered, how it is processed, where it is kept, and who can access it. Clear

comprehension of the data flow is provided by this fundamental stage, which is essential for compliance initiatives.

2. Implement Robust Data Governance Policies-

Create and implement thorough data governance policies that specify how the company will handle personal data. Policies for data collection, processing, storage, and disposal should be part of this. Spread the word about these policies to all staff members and interested parties.

3. Provide Ongoing Employee Training- Organise frequent training sessions to inform staff members of their responsibilities regarding data protection compliance. Make certain that employees are knowledgeable about the Act's requirements, appreciate the value of privacy, and know how to handle personal information responsibly.

4. Obtain Explicit Consent- Prioritise getting people's express, informed consent before gathering and using their personal information. Make sure that people can opt out or withdraw their consent at any time, and that the uses of the data are made clear to them.

5. Implement Strong Security Measures- Put strong organisational and technical security measures in place to guard against breaches, illegal access, and other security incidents involving personal data. This covers the use of secure communication channels, encryption, access controls, and routine security assessments.

6. Establish Data Subject Rights Procedures- Create and put into place processes for responding to requests from data subjects, such as those for data portability, access, rectification, and erasure. Make certain that these requests are handled quickly and in compliance with the Act's specifications.

7. Monitor and Respond to Data Breaches- Establish a strong incident response strategy to find, notify, and handle data breaches. Establish precise procedures for promptly informing impacted parties and regulatory agencies. To find the underlying causes and implement solutions, carry out exhaustive research.

8. Regularly Update Privacy Notices- Update consent forms and privacy notifications to reflect the organisation's current data handling procedures. Make sure people are aware of any modifications to the way their data is handled and give them a chance to check and amend their preferences.

9. Engage Data Protection Officers (DPOs) or Compliance Experts- Think about hiring a data protection officer or consulting data protection-focused compliance specialists. Their knowledge can be quite helpful in navigating the intricacies of compliance and guaranteeing adherence to the requirements of the Act.

10. Conduct Periodic Compliance Audits: Examine and evaluate the organisation's adherence to the Act on a regular basis. To assess adherence to data protection rules and processes, conduct internal audits or hire outside assessors.

Ethical Considerations

In the digital era, data protection and privacy carry profound ethical implications. Balancing the rights of individuals to safeguard their personal information with the potential societal benefits derived from data-driven technologies is a critical ethical challenge¹¹.

¹¹TheHindu,<https://www.thehindu.com/news/national/explained-what-is-the-data-protection-bill-of-2023/article67162906.ece>, (Last visited on November 9th, 2023)

1. **Individual Autonomy and Control-** Respecting individual autonomy is a fundamental ethical principle in data protection. It recognizes that individuals should have agency over their personal information, deciding how it is collected, used, and shared. Upholding this autonomy fosters trust and empowers individuals to participate in the digital landscape without fear of exploitation.
2. **Preventing Harm and Exploitation-** Ethical considerations in data protection extend to preventing harm and exploitation. Mishandling or unauthorised access to personal data can lead to various forms of harm, including identity theft, financial loss, and emotional distress. Ensuring robust data protection measures is imperative in mitigating these risks.
3. **Societal Benefits and the Common Good-**At the same time, ethical deliberations must acknowledge the potential societal benefits that can arise from responsible data use. Data-driven technologies have the capacity to advance scientific research, enhance public services, and drive economic growth. Striking a balance between individual privacy rights and the collective good requires thoughtful consideration and transparent governance.
4. **Transparency and Accountability-** Ethical data protection practices demand transparency and accountability from organisations and institutions. Openly communicating data handling practices, obtaining informed consent, and being transparent about how data is used are crucial components of an ethical data ecosystem.
5. **Mitigating Discrimination and Bias-** Ensuring fairness and equity in data processing is another ethical imperative. Algorithms and automated decision-making systems must be designed to mitigate biases that could perpetuate discrimination based on factors like race, gender, or socioeconomic status.

FUTURE TRENDS IN DATA PROTECTION LEGISLATION¹²

1. **Global Standardisation-** We can anticipate a push for greater global standardisation in data protection laws. Efforts to harmonise regulations across jurisdictions will be crucial as data flows transcend international boundaries.
2. **Enhanced Individual Rights-** Future legislation may expand upon individual rights, potentially introducing new rights related to algorithmic transparency, automated decision-making, and the portability of complex data sets.
3. **Stricter Enforcement Mechanisms-** Regulatory authorities are likely to adopt more stringent enforcement measures, including higher fines for non-compliance. This will incentivize organizations to invest in robust data protection measures.
4. **Focus on Emerging Technologies-** Anticipate a strong focus on regulating emerging technologies like artificial intelligence, blockchain, and IoT devices. Legislation will need to address the unique challenges posed by these technologies in relation to data protection.

¹²CarnegieIndia,<https://carnegieindia.org/2023/10/03/understanding-india-s-new-data-protection-law-pub-90624>(Last visited on November 9th, 2023)

Implications of Emerging Technologies¹³

1. Artificial Intelligence (AI) and Machine Learning- The widespread adoption of AI and machine learning will necessitate new regulations to ensure transparency, accountability, and fairness in automated decision-making processes.
2. Blockchain and Decentralization- Blockchain's decentralised nature offers potential benefits for data security. However, reconciling this technology with the right to be forgotten presents a unique challenge.
3. Internet of Things (IoT)- As the number of IoT devices continues to grow, regulations must evolve to address the security and privacy concerns associated with the vast amounts of personal data generated by these devices.
4. Biometric Data and Facial Recognition- The increasing use of biometric data, particularly facial recognition technology, will require strict regulations to prevent misuse and protect individual privacy.
5. Edge Computing- The rise of edge computing will prompt a re-evaluation of where data is processed and stored. Data protection laws may need to adapt to account for this shift in data processing paradigms.

The future data protection legislation will likely be characterised by global standardisation efforts, enhanced individual rights, and stricter enforcement mechanisms. Additionally, the impact of emerging technologies such as AI, blockchain, IoT, biometrics, and edge computing will play a significant role in shaping the regulatory landscape for personal data protection. Adapting to these trends will be essential for organisations and policymakers alike.

Criticism

The DPDP Act, 2023 intent to protect personal data, but potential challenges in its implementations arises both technically and logically as Section 36 of this act gives expansive authority to central government to request such information from the board or any data fiduciary. Further, the exceptions delineated for consent significantly empower the state and elevate state imperatives above those of private entities and this can be justified by saying that in certain situations, such as disasters or emergencies, the law broadens the scope of such scenarios. For instance, Section 7(b) of the legislation allows the government to bypass consent requirements if a government service beneficiary has previously agreed to receive any other benefit from the state. While this facilitates smoother access to personal data for individuals receiving government services, it also empowers government to bypass the law, they can retain personal information after fulfilling intended use and exempt government from the purpose of limitations.

In case of processing of children's data, Sections 9(1) to 9(3) outline particular requirements, including the necessity for parental consent and the prohibition of profiling. Here also, government gets authority to exempt any business or category of businesses from section Sections 9(1) to 9(3), "subject to such conditions, as may be prescribed." Unfortunately, this provision lacks clarity on the criteria for granting exemptions and the process for determining conditions. The absence of clear guidance raises concerns about the potential misuse of this provision.

¹³PeopleMattersIndia, <https://www.peoplesmatters.in/news/economy-policy/key-highlights-of-digital-personal-data-protection-bill-2023-38671>, (Last visited on November 9th, 2023)

Moreover, Section 17(a) empowers the central government to exempt certain state facts from the stringent provision related to personal data processing. Furthermore section 8(1) (j) of the RTI is amended by this act through Section 44(3) disrupts the delicate balance between and informational rights by expanding the authority of PIO to potentially reject RTI applications citing personal data concerns.

Conclusion

Privacy is a Fundamental right and it is very precious in this digital age, despite the fact it's all about privacy there is no legal definition of privacy is given under DPDP Act, 2023 or any other law in India. It remains debatable and its meaning changes from person to person. Further, consent should be obtained by the data fiduciaries is mandatory before processing the data if a person disagrees to give consent then what will happen? Do he still will be beneficiary. Furthermore, it's all about personal data and what about non-personal data there is nowhere defined in this act that what non-personal data, many provisions in this act exempts government which create dilemma, is it still about protecting data of citizens or just a surveillance system of government. Dark patterns can be combatted but to a limited extent because there is no provisions in this act which directly talks about the Dark pattern. We need more laws related to the way data fiduciaries are going to obtain consent. Moreover, there is problem in structuring of DPB, It operates as an autonomous body with restricted scope, and the government will establish procedures for appointing its members. Although the law defines qualifications for board members, it does not specify the board's composition in terms of the number of members, mandating only one of them to be a legal expert. This particular stipulation presents an issue, given that one of the board's primary responsibilities is to levy penalties and provide directives for noncompliance. The implications of the Act on businesses, government agencies, and non-profit organizations underscore the transformative impact on data management practices. Enhanced data governance requirements, increased accountability, and transparency pose challenges for businesses, while government agencies must allocate resources for compliance. The ethical considerations inherent in data protection underscore the delicate balance between individual autonomy, preventing harm, and realizing societal benefits. The section on ensuring compliance provides a practical roadmap for enterprises, emphasizing the need for comprehensive data audits, robust governance policies, ongoing employee training, and strong security measures. The future trends and challenges in data protection legislation anticipate global standardization, enhanced individual rights, and stricter enforcement mechanisms, while the impact of emerging technologies like AI, blockchain, and IoT will reshape the regulatory landscape. This paper provides a multifaceted exploration of digital privacy, spanning historical context, legal frameworks, ethical considerations, and future trends. As the digital landscape continues to evolve, the delicate balance between innovation and privacy protection remains a critical challenge for legislators, businesses, and individuals alike. The discourse initiated in this paper contributes to the ongoing dialogue on ethical design, responsible data handling, and the quest for a harmonious coexistence in the digital age.