International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Corporate Accountability and Consent Management in AI-Enabled Banking: A Critical Study under the Digital Personal Data Protection Act

L Harika[1], Dr Nagaraja V[2]

[1]LL.M (Business & Corporate Law), School of Legal Studies, Reva University
[2]Professor, School of Legal Studies, Reva University

Abstract

The growing adoption of Artificial Intelligence (AI) in the banking industry has brought about a revolution in the financial sector by making it more efficient, automated, and data-driven in decision-making. Nevertheless, the protection of personal data has also become a major issue with the help of this technological development, especially concerning the corporate responsibility and consent issue. This paper is a critical analysis of the framework provided by the Digital Personal Data Protection Act, 2023 (DPDP Act) regarding the application of AI in banking in India.

The study takes a dogmatic and descriptive stance to assess how efficient legal provisions in conserving the data fiduciaries are and, particularly, how accountable they are in their use of the AI systems in regard to personal data. It also discusses the essence and legality of the consent practices adopted in online banking environments whether such consent is in fact informed and meaningful. The research determines major issues, such as the absence of transparency in the decision-making process by algorithms, low levels of explainability, and formal instead of substantive consent.

The paper delineates the gaps in the current legal framework that necessitate crucial analysis and practical examples and can include deficiencies in the current laws governing AIs, especially the lack of provisions in the legal system aimed at the specific regulation of AI, and the impossibility of holding responsible parties accountable in complicated technological contexts. The results indicate that although the DPDP Act is a great move towards enhancing the protection of data, it still needs some improvements to meet the special risks that the AI technologies represent. The paper ends with the recommendation of stricter accountability principles, more stringent transparency levels, and more efficient sets of consent particularities in order to guarantee the preservation of the rights of individuals in the changing digital banking environment.

Keywords: Artificial Intelligence in Banking, Corporate Accountability ,Consent Management ,Digital Personal Data Protection Act, 2023,Data Fiduciary

1. Introduction

The fast adoption of Artificial Intelligence (AI) in the banking industry has profoundly changed the mode of operation and service delivery by financial institutions. Machine learning algorithms, predictive

analytics and automated decision-making technologies based on AI are being applied to purposes such as credit scoring, fraud detection, chatbots to serve customers and Know Your Customer (KYC) verification[1]. These developments have increased efficiency, lowered cost of operation and improved customer experience. Nevertheless, the massive use of AI systems implies the large-scale data gathering and processing, which is highly problematic in terms of the privacy and protection of the personal data.

In that regard, the issue of personal data protection has become a burning problem, especially with digital banking where financial and personal data is handled continuously with sensitive nature. The introduction of the Digital Personal Data Protection Act, 2023 (DPDP Act) is an important milestone in the Indian attempts to create a coherent framework of legislation in the field of processing personal data. The Act provides requirements on data fiduciaries, such as "banks and other financial institutions, and focuses on principles, such as the legality of the processing, the limitation of purposes, and the consent of the users. It also aims at enabling individuals as known as data principals with rights to their personal data.

Regardless of such regulatory progress, there are still a number of pitfalls in the path of assuring effective corporate accountability and duty-informed consent management in AI-based banking systems. The most concerning one is the inability to make AI-driven decisions transparent, which is known as the black-box problem[2]. There is also the likelihood that the customers are not well informed on how they decide, including whether they approve loan or fraud warnings without lingering questions on fairness, accountability, and the risk of being biased. Besides, consent modalities in online banking are usually so poor or even superficial, and clients would often consent by signing lengthy and cumbersome terms and conditions that they might not have understood effectively.

It is against this background that the current research paper will aim to respond to the following research questions: How effective is company accountability under the DPDP Act in controlling AI-driven banking practices? How effective is the consent management in making sure that there are informed and voluntary user participation in such systems? This study aims at critically analyzing the role of corporate accountability in AI-driven banking, assessing the efficacy of consent mechanisms by the DPDP Act, and the gaps and issues that may arise in the existing law.

This paper is confined to the doctrinal and analytical analysis of the legal and regulatory implication of corporate responsible behaviour and consent management in the Indian banking industry. It pays specific attention to the consequences of AI technologies according to the DPDP Act, 2023. The study however, is not conducted on the basis of the collection of empirical data or technical examination of AI systems. Although it might attract few comparisons with the global systems, its main target is the Indian legal system.

2. Conceptual Framework

Throughout the research, I have developed a conceptual framework based on three main pillars, which include Artificial Intelligence in banking, corporate accountability, and consent management[3]. These concepts are important to understand in order to analyze critical legal and regulatory issues concerning AI-enabled financial systems with the required degree of criticism.

[1] Wani NU, Hamza N, Saboori B. Legal and Ethical Frameworks for AI in Financial Services: Balancing the Innovation with Responsibility and Effective Protection. InGreen Horizons: Role of AI in Sustainable Finance 2025 Jul 22 (pp. 177-196). Singapore: Springer Nature Singapore.

[2] Omotoso O. Financial Exclusion in Modern Banking: A Legal Analysis of Accountability and the Right to Explanation in AI-Driven Decision Systems. Available at SSRN 5743224. 2025 Nov 11.

[3] Michael D. Data Privacy Concerns and Ethical Issues in AI-Driven Financial Services.

The Artificial Intelligence in Banking has been taken to mean the advanced computational systems which are capable of doing tasks that are typically the prerogative of human intelligence such as learning, reasoning and others that all involve decision making. Machine learning, a subdivision of AI, allows systems to process vast amounts of data and extract patterns to either make predictions or decisions without necessarily being coded. Applications of AI to an area of the banking industry include credit scoring, where algorithms determine how creditworthy a person is by taking into account their financial behavior in real-time; fraud detection, where anomestic patterns in transactions can be detected in real-time; and customer service, where chatbots asynchronously provide automated customer support. These apps are highly dependent on the use of algorithms, the personal and financial information in processing and providing the results, which directly influence individuals.

In the context of data protection, corporate accountability means that it is the responsibility of organizations to ensure that personal data is used in a lawful, fair and transparent way. According to the DPDP Act, the banks and other financial institutions are defined as data fiduciaries, by which they are legally obliged to ensure the safety of personal data of people and adhere to the ideas outlined in the Act. This involves proper technical and organizational actions, data security and responsibility to misuse or data breach. Corporate responsibility turns out to be especially relevant in AI-based contexts, where automated systems can deliver the results that are hard to read or criticize, thus enhancing the necessity of regulation and accountability.

Another significant aspect of the conceptual framework is consent management as it is the basis of the legalization of processing personal data under the DPDP Act. The informed consent stipulates that the persons should be given clear and comprehensive information on the use of their data and then they have to make a decision[4]. The consent should be free, that is, should not be by coercion or undue influence, specific, that is, should refer to a very specific purpose, and unambiguous, so that it is misinterpreted. Also, it is necessary that people should be able to revoke their consent. Practically, though, consent management in digital banking is often challenged by such factors as the complicated privacy policy, absence of awareness among the users, and the inability to comprehend AI-based processes. Such problems make one wonder whether the consent given under such circumstances can be regarded as valid and effective at all.

These ideas are collectively taken as the basis of the study of interaction between technology, law, and rights of the individual, in the context of AI-based banking.

3. Legal Framework: Digital Personal Data Protection Act, 2023

3.1 Major characteristics of the DPDP Act.

Digital Personal Data Protection Act, 2023 (DPDP Act) is a full-fledged law that was put forth to govern the handling of personal data in India. Making obligations on items that fall under the category of data fiduciary is one of its core qualities that involve banks and other financial institutions. Such obligations demand that data fiduciaries should process personal data fairly, in a legal way, and transparently and at the same time making it accurate and safe. They also have the obligations to use proper technical and organizational controls to avoid data breach and unauthorized access[5]. Secondly, it is possible that

[4] Gupta A, Amarnani M, Soanki S, Kishore J. AI and data privacy in business. In2025 First international conference on advances in computer science, electrical, electronics, and communication technologies (CE2CT) 2025 Feb 21 (pp. 109-114). IEEE.

[5] Sundara K, Narendran N. The Digital Personal Data Protection Act, 2023: analysing India's dynamic approach to data protection. Computer Law Review International. 2023 Oct 1;24(5).

significant data fiduciaries will have higher compliance obligations like data audits, data protection officers.

The other prominent aspect of the Act is that it has the right to the data principal i.e. the person whose personal data is being handled. They have such rights as the right to obtain detail of the way their data are processed, the right to correct and destroy erroneous or obsolete data, and the right to seek redress of grievances. The Act also grants the right of the individuals to revoke consent therefore giving them greater control of their personal information. These rights are also fundamental in making sure that individuals are not pass-on in the data processing ecosystem but being participants of it.

The DPDP Act is based on the concept of consent. The consent as required by the Act must be free, specific, informed, unconditional and does not have any conditions two, must be unambiguous with the agreement being clearly expressed through a clear affirmative action. Fiduciary of the data must make a clear notification of the interest of data gathering and the method the information is to be utilized. Moreover, the principle of user autonomy should be supported by the fact that consent should be easy to revoke as easy to grant. These are the provisions, which are critical especially in digital settings where people tend to deal with automated systems.

3.2. Relevant Provisions to the AI Banking.

Some provisions provided in the DPDP Act are especially applicable to banking systems based on AI. The notice and consent are one of the most crucial ones. Banks have a duty to give notices to individuals in a clear and understandable manner before a personal data is processed giving the nature of the data being collected, the intended use of the data as well as the rights that individuals have over it[6]. Considering the field of AI, where many decisions are likely to be automated and complicated, it is a vital requirement that would contribute to transparency and awareness of the users.

Another important provision is the principle of purpose limitation. It states that individual data should be gathered on account of definite, legitimate objectives but not be utilized in behavior of actions not allied with original consent. This principle becomes necessary in AI-based banking when the use of data can be repurposed by analytics or predictive models this is necessary to avoid the misuse of data and unauthorized secondary use.

Data reduction also supports the defensive framework as it requires that the information must be collected and processed in terms of its necessity to the intended goal[7]. This is especially applicable in systems of AI which usually involve large amounts of data since it limits the unscrupulous amassing of personal data.

The provisions of the Accountability included into the Act promote the idea of accountability of data fiduciaries, so that even the current case of third-party data processing or automation cannot escape obligations to comply with all the mandated legal requirements. The banks need to prove that they have undertaken sufficient actions to secure the data, as also to adhere to the stipulation of the Act. This involves record keeping, risk evaluation, and making sure that AI systems are applied within the sphere of the law of fairness and transparency.

3.3. Data Protection Board Responsibility

The Data protection board of India is also very vital in the implementation of the DPDP act. It has the authority to check the compliance, and define violations as well as settling the disagreements that may

[6] Naithani P. Analysis of India's digital personal data protection act, 2023. International Journal of Law and Management. 2025 Aug 26;67(5):543-53.

[7] Bareh CK. Reviewing the Privacy Implications of Indias Digital Personal Data Protection Act (2023) from Library Contexts. DESIDOC Journal of Library & Information Technology. 2024 Jan 23;44(1):50-8.

occur due to the breach of the Act[8]. Board can be considered as a regulatory force that should also assure that the data fiduciaries do not breach their duties and that they do not violate the rights of data principals. The Board can carry out severe financial punishments on defaulting entities in case of non complaisance. These sanctions are set to serve as a reminder on fear of carelessness and abuse in data processing. The Board can also provide instructions to cause corrections like to stop some data processing activities or take tighter protection.

AI-enabled banking involves the use of the Data Protection Board that is vital in enforcing all the regulations concerning the threat of breaching the values and principles of banking. It is critical to its effectiveness in keeping the digital financial ecosystem trustworthy because it oversees accountability and compliance.

4. Corporate Accountability in AI-Enabled Banking

4.1 Obligations of Banks as Data Fiduciaries

With banking being AI-enabled, corporate accountability gains an extra relevance because of the intricacy and magnitude of data processing. Banks are the data fiduciaries they must implement sound risk management processes to recognize and curb possible harms relating to the use of the AI systems under DPDP Act[9]. This covers the evaluation of risks in relation to the data breach, errors in algorithms, and abuse of personal information. The deployment and creation of AI technologies need to have effective risk management structures so that they are used in a safe and sound way.

Another important requirement that banks have is transparency. They must ensure that they present simple and readable information to the customers on the treatment of their personal information. The application of AI in this way involves clarifying the reasoning which lies behind automated decision-making activities to the best of its ability. That is not only will transparency help build trust but also allow individuals to make informed decisions regarding their data.

The issue of algorithmic accountability is a recent development of corporate responsibility, especially in AI-driven systems. Banks should make sure that their algorithms do not develop unfairly and selectively. This includes testing, validating and auditing AI models regularly to identify and address biases or inaccuracies. There should also be systems to deal with the complaints that are a result of automated decisions like wrong credit assessment or false fraud notices.

4.2 Issues and Challenges

Nevertheless, there are a number of issues that impede proper execution of corporate accountability in AI-enabled banking despite the legal structure. Among the most severe ones, one can single out the fact that black-box AI systems attack is prevalent: even experts might not easily comprehend the internal mechanics behind algorithms[10]. Such insider trading allows carrying out of business transactions with risk of not understanding how the decision to adopt a particular method is made and whether it is subjugated to the lawful and ethical criteria.

Almost similar to this issue is the lack of explainability problem. Automated decisions on customers are usually explained inadequately and hence customers are not empowered to appeal or challenge the

[8] Gupta N, George A. Digital Personal Data Protection Act, 2023: Charting the Future of India's Data Regulation. InData Governance and the Digital Economy in Asia 2024 Dec 31 (pp. 34-53). Routledge.

[9] Bokka VV. Transforming US banking: Leveraging AI-powered technology compliance platform (TCP) for regulatory excellence.

[10] Whitetaker K, Kemp M. The Impact of AI-Enabled Decision Support Systems on Operational Efficiency in Banking Institutions. Available at SSRN 5442594. 2025 Sep 4.

decisions. This also brings the issue of fairness and due process especially in matters that are of a high financial cost.

Another issue relates to AI systems, which is prejudice and discrimination. An algorithm that is learned using historical data is likely to recreate and keep the existing social and economic biases, hence will produce discriminative results. An example is that he or she can deny some groups the credit they deserve or subject them to more scrutiny by a fraud detection system. These problems show the shortcomings of using automated processes without the monitoring of a person.

4.3 Critical Analysis

Although DPDP Act may be said to offer a baseline of how corporate accountability may be carried out, its usefulness in resolving the challenges that arise with the adoption of AI-enabling banking is minimal. The Act mainly centered on the data protection concepts, including the consent, the purpose limitation, and security, yet it fails to mention the specific risks of AI systems, including the presence of bias in the algorithm and absence of explanability.

In addition, the fact that no specifications are given regarding the transparency and accountability of the algorithms promotes regulatory gaps[11]. The data fiduciaries are bound to adhere to the formal requirements but not necessarily provide substantive fairness in their operations which are carried out with the help of AI. The implementation tools, notwithstanding their importance, also can be practically problematic with regards to finding and dealing with breach within intricate technological settings.

Thus, even though the DPDP Act is a significant move to enhancing data protection and corporate responsibility, additional regulations and guidelines that are more specific to the effects of AI in banking are necessary. More effective monitoring, better guidelines, and more focus on ethical applications of AI are required so that the technological progress does not liability to the individual rights and justice.

5. Consent Management in AI-Based Banking Systems

5.1 Nature of Consent in Digital Banking

In digital banking systems, consent is a key element in the processing of personal data legitimation. Consent is frequently acquired with the assistance of digital interfaces in modern banking practice, usually in click-based consent mechanisms. Such systems make users consent to terms and condition or privacy policies by clicking at the option of agreement like, I agree or Accept. Although this approach proves to be effective and open to scaling, there is a question of whether this kind of consent is truly informed and meaningful[12]. On the internet, users often sign the agreement without reading and comprehending what the lengthy and complex agreements state and subsequently consent has been diminished to a formality instead of a substantive protection.

The other relevant point of consent in the digital banking is implied and explicit consent. Implied consent is presumed by what a user does (that is they keep using a service), whereas explicit consent is provided by an express and definite action that indicates consent. In AI-powered banking, where sensitive financial information is being operated with, making automated decisions, explicit consent is deemed as more suitable since it guarantees a better level of user awareness and control. In reality, however, most banking services are based on implied consent or bundled consent, where there is more than one purpose within

[11] Oksanen J. Balancing the Impact of AI-enabled Customer Experience in Banking Sector.

[12] Ahmed A, Shah A, Ahmed T, Yasin S, Longa FE, Hussaini W, Zubair M. AI-Driven Innovations in Modern Banking: From Secure Digital Transactions to Risk Management, Compliance Frameworks, and AI-Based ATM Forecasting Systems. Journal of Management Science Research Review. 2025 Sep 6;4(3):1145-83.

one and the same overall agreement, thus blurring the specificity and clarity necessary to make the consent valid.

The consent concept of digital banking is additionally complicated by the fact that AI systems are introduced, and they process data in a manner that could not be easily comprehended by the client. In comparison to the standard process of data processing, the AI process is associated with continuous learning and adaptation of information, and this aspect implies that the goals and consequences of using data can change over time. This dynamic character is a challenge to the old fashioned concept of consent that normally depends on well established and undynamic purposes. Consequently, it becomes more hard to make sure that the consent is valid and informed during the lifecycle of data processing.

5.2 Challenges

Lack of really informed consent is one of the greatest issues in the consent management in AI-based banking systems. Even though the legal frameworks stipulate the need to inform the user about the issues at hand in a clear and comprehensive manner, the fact is that the majority of privacy notices are long, technical, and hard to understand[13]. This would cause information asymmetry between the banks and the customers, in which the users might not have full insight into the manner in which their information is being gathered, processed, or distributed. Therefore, the informed and meaningful consent may not be achieved when such conditions are introduced.

The problem is further complicated by the fact that AI systems are quite complex. Artificial intelligence processes can also include several layers of data analysis, such as predictive modeling and algorithmic decision-making, that can hardly be explained in the straightforward terms. A customer can agree to the utilization of his or her data in credit evaluation, as an example without knowing the weighting ratio of different data points or how decisions are made out of them. Such a deficiency in transparency compromises the issue of informed consent and restricts the freedom of people to make independent decisions on their data.

Another severe issue in digital banking situations is consent fatigue. Customers often have to agree to many services and transactions, and this makes them prone to the desensitization of consent requests. This can have the effect of people approaching terms as the norm, when it comes to their terms and conditions without looking into them and thus undermining the protective role of consent mechanisms. This fact is especially concerning in AI-enabled systems where stakes are higher as a result of the consequences of the automated decision of people on the financial and personal relationships.

Also, a problem of a withdrawal of consent brings practical challenges. Even though this right to withdraw consent is frequently guaranteed by legal frameworks, its application in AI-based applications may be complicated. The data might have been processed already, incorporated into models or provided to third parties and it is difficult to undo the impacts of earlier consent fully. This casts doubts on the usefulness of consent as a control tool in dynamic and data-intensive settings.

5.3. Evaluation under DPDP Act.

The Digital Personal Data Protection Act, 2023, has created a strong framework of managing consent by stating that the consent must be free, specific, informed, unconditional, and unambiguous. It also stipulates that the consent should be given under an apparent affirmation and that people should be in a position to withdraw the consent as easy as giving the consent. Although the provisions portray high-quality standards

[13] Adari VK. Building trust in AI-first banking: Ethical models, explainability, and responsible governance. International Journal of Research and Applied Innovations. 2021 Mar 10;4(2):4913-20.

on normativity, there are a number of challenges when their practical application is adopted in the AI-enabled banking systems.

A major issue that has been raised is whether the consent that is received in the digital banking situations can really be termed as informed[14]. Considering that AI systems are often complex, and the processing of the data is rather technical, it is hard to be sure that their users are completely aware of the consequences of their consent. Even in cases where the banks deliver detailed notices, the impact of the notices on the users is bound by the capacity and interest of users to dig the relevant information. Consequently, a disparity exists between the legal principle of informed consent and the code of practice regarding the users.

Moreover, specificity might not be an easy parameter to meet in AI-based settings where information is employed in various and dynamic roles. Banks will not necessarily be able to outline every possible application of the data when it is being collected hence they will ask the customer to provide broad or vaguely defined consent which does not necessarily adhere to the legal standards. This puts in conflict a demand on innovation, and on demanding accurate and transparent data practices.

There are also practical challenges with the implementation of the withdrawal of consent. Although the DPDP Act focuses on user control, the technical structure of AI systems might not be easily drawn to fully eliminating the data after they are incorporated in the models or analytics processes[15]. This weakness obstructs the usefulness of consent as a means of continued regulation of personal data.

Finally, as much as DPDP Act offers a powerful legal basis to consent management, the efficiency of such a regulatory process within the framework of the AI-based banking service relies on the quality of the implementation of these principles. The simplified consent processes, increased transparency, and the creation of user-friendly methodologies that may improve the understanding and control is needed. In the absence of such, consent will only be one of the formalities of the process instead of a practical protector of the rights of individuals.

6. Comparative Analysis

The Digital Personal Data Protection Act, 2023 may be compared to the international regulations to find a solution, especially the General Data Protection Regulation (GDPR) of the European Union in this case because both systems are fundamentally different in the area of corporate responsibility and consent manipulation[16]. The GDPR is commonly referred to as one of the most detailed data protection regimes across the world that provide more robust security and elaborate claims in the regulation of data processing each and every activity.

The liability of the GDPR is that there is an accountability focus. It deems data controllers not just to adhere to the law, but also to express a evidence of compliance by way of documentation, impact assessment and frequent auditing. Data protection by design and by default is the notion that the concept of privacy is considered as the development of the systems. Conversely, although the DPDP Act places the responsibility on data fiduciaries, it does not give comprehensive specifications on active responsibility measures, especially the AI systems.

[14] Rao VN, Vijayasimha N. Why Privacy Laws Fail or Succeed: Cost, Architecture, and Governance under the DPDP Act in Comparative Perspective.
[15] Kumar D. The Right to Privacy Under Article 21: Implications of the DPDP Act, 2023 for Data Protection in India. IJLRP-International Journal of Leading Research Publication.;6(8).
[16] Gupta H, Dave DB. [In] Adequacy of the DPDP Act vis-a-vis Right to Privacy at Workplace. NUJS J. Regul. Stud.. 2025;10:57.

The GDPR has a very high standard on consent framework in that it demands that consent should be clear, informed, and specific with an explicit ban on pre-ticks and implied consent. It also states the significance of granular consent by which it is possible to accept various forms of data processing individually. Also, given that automated decision-making has the right to be informed, the GDPR grants people in some instances, the right to request a human intervention. These are additional clauses that improve transparency and empower the users in AI-driven settings.

The DPDP Act has some of the same principles but the prone is relatively lax in some areas. As an example, it does not specifically deal with such problems as the transparency of the algorithm or the right to explain in automated decision-making[17]. This poses a regulatory loophole with regards to the AI-driven banking, in which these safeguards are essential.

The accountability and the user rights are also put forward in other international frameworks, including those that are used in other countries such as Canada and Australia, and usually include rules on the ethical use of AI. These frameworks emphasize the increased realization of the need to control not only the data processing but also technologies based on such data.

Comprehensively it can be seen that although the DPDP Act is a big step in improving protection of data in India, there could be improvement with regard to making it fit in into best practices in the global system. Increasing accountability levels and perfecting the consents systems, especially concerning AI systems would help prepare a tighter and more efficient regulatory regime.

7. Case Studies

The problems of corporate responsibility and consent management in AI-driven banking can be interpreted more clearly in terms of the judicial and regulatory rulings that shed light on the legal framework underpinning the data protection and privacy as well as automated decision-making.

One of the landmark cases in Indian history is the case of Justice K.S. Puttaswamy v. Union of India where the Supreme Court established the right to privacy as a fundamental right under the Constitution of Article 21. The Court highlighted that the right to informational privacy and control of personal data is fundamental to personal autonomy. This ruling is the constitutional basis of the contemporary data protection regulations, such as the DPDP Act, 2023. This scenario highlights in the context of banking with AI-enabled services that any automated manipulation of personal financial information should ensure a respect to the user consent, transparency, and proportionality.

Google LLC v. Competition Commission of India is another notable case, in which the Competition Commission of India (CCI) found Google guilty of abusing dominant position in the Android ecosystem. The lack of user choice, forced consent, and exploitation of data stood out as some of the issues noted in the case[18]. The decision is very applicable to AI-based banking since it shows how online platforms may set unreasonable terms and obtain consent in an opaque fashion, thus compromising meaningful user autonomy.

The Court of Justice of the European Union (CJEU) decision in the Schrems II Case (Data Protection Commissioner v. Facebook Ireland Ltd.) is essential on the international level. The Court struck the EU-

[17] Bharanitharan K, Kaur G. A Comparative Analysis of Data Minimization Principles: Evaluating GDPR and India's DPDP Act 2023. InInternational Conference On Data Mining And Information Security 2024 Oct 6 (pp. 41-55). Singapore: Springer Nature Singapore.

[18] Bisht AK, Sreenivasulu NS. Information Privacy Rights in India: A Study of the Digital Personal Data Protection Act, 2023. InData Privacy-Techniques, Applications, and Standards 2024 Nov 29. IntechOpen.

US Privacy Shield framework because of insufficient data protection rights and reiterated the need to have an effective control on personal data. The case implies that powerful accountability frameworks and enforceable data protection criteria are needed, which are also applicable to AI-based financial systems that process cross-border data flows.

Likewise the State of Wisconsin v. Loomis case depicts the uncertainties of using algorithms in decision-making. There were concerns regarding transparency, bias, and explainability when a risk assessment algorithm was used in criminal sentencing. Though the court did not prohibit its use, they recognized the drawbacks of algorithmic opaqueness. This scenario is parallel to credit scoring systems that are based on AI and used in the banking sector, as the decisions that impact people are not explained, which is a factor of accountability.

The other regulatory development of interest is the move by the European Commission in the Google Shopping Case where Google was fined on grounds of preferring its services in search results. The case underscores the distortion of fairness and competitiveness by the algorithmic systems. With AI in banking, the same risk exists as certain customers or results are favored by the algorithms, without being transparent, which can result in discriminatory actions.

All these case laws go to show that though technology is an efficiency booster, it also poses some serious questions on transparency, fairness and accountability. They reinforce the necessity of ensuring tighter regulatory controls, explicit consenting procedures, and enhanced explainability of algorithms in AI-based banking systems. Although the Indian DPDP Act, 2023, is progressive, it still needs to develop more to integrate these principles to achieve maximum impact in handling the emerging technological challenges.

8. Findings and Discussion

Corporate responsibility and consent control in AI-based banking as stipulated by the Digital Personal Data Protection Act, 2023 were analyzed, which presented a number of significant conclusions. The poor enforcement mechanisms are one of the main findings. The fact that the Act provides a regulatory framework and penalties does not mean much since the effectiveness of the Act is highly dependent on the ability of the enforcement authorities to pay attention to the observance of compliance and deal with the breach of the act. The practical implications of the law may be restricted by the fact that it is especially difficult to identify violations and hold them accountable in complex AI-driven environments since such software can be effectively used to monitor multiple areas.

The other important discovery is the lack of provisions that are specific to AI in the Act. Although the values of the DPDP Act are general principles of data protection, it is not sufficient in particular issues concerning AI technologies, including the question of bias in the algorithms, their inexplicability, and the autonomous character of decisions made by these algorithms[19]. This regulation loophole leaves things unclear and gives data fiduciaries a wide-range in which they can operate, without being limited to particular and customized rules of AI systems. Consequently the problem of fairness, transparency and accountability are not adequately looked into.

The paper also puts emphasis on the fact that consent in its current application in digital banking is more than formal but not substantial. The fact of the matter is with the Act being more focused on informed and explicit consent, in most instances users give consent without having a full understanding of the repercussions. This is caused by such factors as a complicated privacy policy, information overload, and

[19] Hanspal MS. The Digital Personal Data Protection Act, 2023: Key Provisions, Issues, and Future Directions. DME Journal of Law. 2025 Dec 31;6(2):12-23.

consent fatigue. As a result, the consent mechanisms do not serve such an important role of empowering people and protecting their rights.

Besides, the interaction of the technological complexity and the legal requirements brings in more challenges. The AI systems work in dynamic and changing modes and it is hard to ascertain that they will comply with the unchanging legal provisions consistently. This deficiency in linking law and technology highlights why there is a need to adopt responsive regulation. On balance, the results indicate that the DPDP Act is a good measure to enhance data protection, but it still needs improvement and introduction of an efficient system to accommodate the AI-facilitated banking.

9. Suggestions / Recommendations

To solve the challenges identified, it is necessary to propose AI-related regulations that determine clearly the responsibility of the automated system of decisions. The necessity to have algorithmic transparency and explainability can lead to a higher level of trust and allow human beings to comprehend and dispute decisions. The consent frameworks must be brought to the simplest form and allow making them more user-friendly so that the consent could be properly informed and meaningful. The audits and impact evaluation of AI systems should be carried out regularly to identify biases as well as keep AI systems within the legal framework. Also, the awareness of the consumer of the rights to the data and the privacy in the online sphere may provide them with the capacity to make the right decisions and reinforce the overall performance of the regulation system.

10. Conclusion

This paper has discussed the problems of corporate responsibility and consent management in AI-based banking in the Digital Personal Data Protection Act, 2023. It pointed out that as much as the Act is a base element in data protection there are a lot of hurdles to overcome in the issue of dealing with the complexity of the AI systems. Among the most important issues are transparency deficiency, ineffective consent practices as well as inadequate regulation. The final assessment of the analyzed article is that DPDP Act, which is such an advancement, lacks the necessary tools to enforce control over AI-based practices. Thus, the urgent changes that would include AI-related clauses and enhance the mechanisms of accountability and consent should be made to secure the safety of personal rights.

Reference

1. Wani NU, Hamza N, Saboori B. Legal and Ethical Frameworks for AI in Financial Services: Balancing the Innovation with Responsibility and Effective Protection. InGreen Horizons: Role of AI in Sustainable Finance 2025 Jul 22 (pp. 177-196). Singapore: Springer Nature Singapore.
2. Omotoso O. Financial Exclusion in Modern Banking: A Legal Analysis of Accountability and the Right to Explanation in AI-Driven Decision Systems. Available at SSRN 5743224. 2025 Nov 11.
3. Michael D. Data Privacy Concerns and Ethical Issues in AI-Driven Financial Services.
4. Gupta A, Amarnani M, Soanki S, Kishore J. AI and data privacy in business. In2025 First international conference on advances in computer science, electrical, electronics, and communication technologies (CE2CT) 2025 Feb 21 (pp. 109-114). IEEE.
5. Sundara K, Narendran N. The Digital Personal Data Protection Act, 2023: analysing India's dynamic approach to data protection. Computer Law Review International. 2023 Oct 1;24(5).

6. Naithani P. Analysis of India's digital personal data protection act, 2023. International Journal of Law and Management. 2025 Aug 26;67(5):543-53.
7. Bareh CK. Reviewing the Privacy Implications of Indias Digital Personal Data Protection Act (2023) from Library Contexts. DESIDOC Journal of Library & Information Technology. 2024 Jan 23;44(1):50-8.
8. Gupta N, George A. Digital Personal Data Protection Act, 2023: Charting the Future of India's Data Regulation. InData Governance and the Digital Economy in Asia 2024 Dec 31 (pp. 34-53). Routledge.
9. Bokka VV. Transforming US banking: Leveraging AI-powered technology compliance platform (TCP) for regulatory excellence.
10. Whitetaker K, Kemp M. The Impact of AI-Enabled Decision Support Systems on Operational Efficiency in Banking Institutions. Available at SSRN 5442594. 2025 Sep 4.
11. Oksanen J. Balancing the Impact of AI-enabled Customer Experience in Banking Sector.
12. Ahmed A, Shah A, Ahmed T, Yasin S, Longa FE, Hussaini W, Zubair M. AI-Driven Innovations in Modern Banking": From Secure Digital Transactions to Risk Management, Compliance Frameworks, and AI-Based ATM Forecasting Systems. Journal of Management Science Research Review. 2025 Sep 6;4(3):1145-83.
13. Adari VK. Building trust in AI-first banking: Ethical models, explainability, and responsible governance. International Journal of Research and Applied Innovations. 2021 Mar 10;4(2):4913-20.
14. Rao VN, Vijayasimha N. Why Privacy Laws Fail or Succeed: Cost, Architecture, and Governance under the DPDP Act in Comparative Perspective.
15. Kumar D. The Right to Privacy Under Article 21: Implications of the DPDP Act, 2023 for Data Protection in India. IJLRP-International Journal of Leading Research Publication.;6(8).
16. Gupta H, Dave DB. [In] Adequacy of the DPDP Act vis-a-vis Right to Privacy at Workplace. NUJS J. Regul. Stud.. 2025;10:57.
17. Bharanitharan K, Kaur G. A Comparative Analysis of Data Minimization Principles: Evaluating GDPR and India's DPDP Act 2023. InInternational Conference On Data Mining And Information Security 2024 Oct 6 (pp. 41-55). Singapore: Springer Nature Singapore.
18. Bisht AK, Sreenivasulu NS. Information Privacy Rights in India: A Study of the Digital Personal Data Protection Act, 2023. InData Privacy-Techniques, Applications, and Standards 2024 Nov 29. IntechOpen.
19. Hanspal MS. The Digital Personal Data Protection Act, 2023: Key Provisions, Issues, and Future Directions. DME Journal of Law. 2025 Dec 31;6(2):12-23.