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

Automated Decision-Making and Individual Rights: A Critical Analysis of Human Intervention under the Digital Personal Data Protection Act, 2023

Niharika Nirmohi[1], Prof. (Dr.) Deepti Monga[2]

[1]LLM Student, University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India
[2]Professor, University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India

Abstract
The use of AI and algorithmic systems in governance, finance, health and work has radically reshaped decision-making about people. Although automated decision making can make institutions more efficient and scalable, it brings about new acute challenges of algorithmic opacity, deep-rooted bias, and loss of human dignity. In the backdrop of this, the present research paper critically reviews the legal framework of India outlined in Digital Personal Data Protection Act, 2023 and Digital Personal Data Protection Rules, 2025 with a particular emphasis on the lack of a standalone statutory right against solely automated decision-making and a right to a human intervention. Adopting a doctrinal and comparative legal research methodology, the study examines the Indian data protection regime's statutory provisions and the jurisprudence of the right to privacy and procedural fairness and compares it with Article 22 of the EU GDPR and Article 14 of the EU AI Act. While Section 8(3), Section 10 and Section 13 of the Digital Personal Data Protection Act, 2023, together with Rule 13 of the Digital Personal Data Protection Rules, 2025, impose obligations of indirect compliance with the rules regarding data accuracy, algorithmic due diligence, and grievance redressal, they do not give individuals the power to challenge automated decisions or to request meaningful human intervention. This paper works towards the view that the legislative and regulatory reforms on targeted measures are necessary to make substantive human-in-the-loop safeguards a part of Indian data protection jurisprudence.

Keywords: Automated Decision-Making, Data Principal Rights, Digital Personal Data Protection Act 2023, Human Intervention, Algorithmic Accountability, Right to Explanation

1. Introduction

Increasingly, automated decision-making systems, relying on machine learning, predictive analytics, and profiling algorithms are used in modern governance and commercial enterprises for the allocation of credit, screening of job applicants, insurance premiums and public welfare subsidies. While algorithmic automation offers speed, uniformity and lower business operations expenses, it also poses significant constitutional and legal questions about allowing complex calculations to determine human life. If a machine decides not to loan an individual money, or not to hire an individual, or not to allow an

individual to apply for state benefits because it has no clear reason for doing so, and the machine works without humans to check this decision, the person is not a "bearer of rights," but a passive data object.

The nine-judge bench of the Supreme Court of India in Justice K. S. Puttaswamy (Retd.) and Another v. Union of India and Others (2017) had recognized informational self-determination, human dignity, and decisional autonomy as fundamental attributes of Article 14, 19, and 21 of the Constitution of India [1]. The Parliament of India has passed the Digital Personal Data Protection Act, 2023 [2] on 11 August 2023 and notified the Digital Personal Data Protection Rules, 2025 [3] on 13 November 2025, pursuant to this constitutional obligation and as recommended by the Committee of Experts chaired by Justice B. N. Srikrishna [4].

Although the Digital Personal Data Protection Act, 2023 is India's first comprehensive statutory data privacy law, it appears to be a minimalist, principle-based legislative approach [5], [6], and is significantly different from international data privacy laws and regulations concerning algorithmic governance [7]. The Indian statute has no explicit obligations on the Data Principal to be excluded from a decision solely on the basis of automated processing, nor does it provide any enforceable rights of the Data Principal to either be provided with the opportunity to express his point of view to the automated processing system, or to challenge the algorithmic outcome [2]. The statutory omission is significant as automated systems are fast gaining traction in the public and private sector in India today.

The main aim of this research paper is to carefully consider whether the rights and obligations provided by Digital Personal Data Protection Act, 2023 and Digital Personal Data Protection Rules, 2025 are sufficient to safeguard individuals against purely automated decisions, or that the lack of a right to human intervention vitiates the constitutional right to due process and informational privacy.

2. Literature Review and Research Methodology

2.1 Review of Existing Literature

The discussion of automated decisions and data protection has developed more or less in an European context. Sandra Wachter, Brent Mittelstadt, and Luciano Floridi (2017) explored the meaning of Article 22 and Recital 71 of the General Data Protection Regulation, showing that although the post-hoc right to an explanation is not explicitly clear in the text, Article 22(3) provides a useful procedural baseline by affirming the right to obtain human intervention and the right to contest only automated decision-making [8]. Lilian Edwards and Michael Veale (2018) also proposed that explanations of complex, black box algorithms are seldom technically satisfactory unless complemented by accountabilities at the structural level and in-depth human scrutiny [9].

In the Indian context, previous drafts of legislation showed a greater degree of engagement with algorithmic risks. In particular, the Committee of Experts on a Data Protection Framework for India (2018) discussed the harm caused by automated profiling and suggested measures for transparency and accountability in the case of important data fiduciaries [4]. Later drafts, such as the one which culminated in the Digital Personal Data Protection Act, 2023, have not included explicit provisions pertaining to automated decision making [6], [10]. As noted by Teesha and Dhawal Shankar Srivastava (2025), the absence of an explicit right to an explanation and human review in the 2023 Act is a greater accountability gap, where formal adherence to the law takes the place of substantive rights [11]. Although the general lack of regulation on artificial intelligence in India is recognised, there is a dearth of a doctrinal analysis focused on how the recently notified Digital Personal Data Protection Rules, 2025

interact with indirect statutory duties under the provisions of Sections 8, 10, 13 in filling or otherwise the gap in human intervention.

2.2 Research Methodology

For this study, the method used is doctrinal, analytical and comparative legal research. The statutory text of the Digital Personal Data Protection Act, 2023, Digital Personal Data Protection Rules, 2025, Constitution of India, Judicial pronouncements of the Supreme Court of India, Regulation (EU) 2016/679 (General Data Protection Regulation), and Regulation (EU) 2024/1689 (European Union Artificial Intelligence Act) have been used as primary sources [1]–[3], [7], [12]. Peer-reviewed legal journals, policy reports and legislative briefs are considered secondary sources [4]–[6], [8], [11].

3. Conceptual Framework: Automated Decision-Making and the Right to Human Intervention

Automated decision-making is the process of making a determination that impacts on an individual that is performed without meaningful human involvement by a technical system and often involves algorithmic profiling of personal characteristics like credit history, trustworthiness, actions or location. In modern machine learning systems, these systems are usually operating as "black boxes" whose inner workings of how variables get weighted together is not easily comprehensible by an operator or by a citizen.

There are three types of risks created by unrestricted automated decision making processes. One, the algorithmic systems, trained on historical datasets, are bound to learn and carry forward casteism and gender, religious and socio-economic discrimination that exists in society. Second, automated profiling erodes individual agency as it evaluates people based on statistical patterns that are derived from group behaviors, and not on individual merits or situations. Third, there is a legal responsibility gap when the algorithm harms the individual: when the algorithm harms, institutions often shift responsibility to technical neutrality, and there is no one to whom to hold the individual accountable.

Modern data protection jurisprudence is based on the idea of human intervention, often expressed as human-in-the-loop or human-on-the-loop governance models, which aim to address these harms. If somebody is to be involved in this process in a meaningful way, it is not enough merely to rubberstamp something with a clerical stamp. In the comparative frameworks of artificial intelligence governance, as stated, human supervision has legal value if it can be claimed that the human individual has the capacity, expertise, and technical means to cancel and/or change the AI output, to review it, and to take into account the external context that the individual can access and consider on their own [12].

4. Legislative Evolution and Statutory Architecture of the Digital Personal Data Protection Act, 2023

4.1 Evolution from the Srikrishna Committee to the 2023 Act

The laws passed by India for a data protection law between 2018 and 2023 did not offer enforceable rights regarding algorithmic decisions. Srikrishna Committee Report (2018) has already recognized that automatic processing and profiling involve some serious concerns regarding the autonomy of the individual, but preferred an accountability regime for the data fiduciaries with review by humans and even to court, rather than granting the individual a right to object to decisions made purely by automatic processing, or a right to a human intervention [4]. The Personal Data Protection Bill, 2019, however, did not give a right to not be the subject of automated decision making [10]. After the notification and enactment of the Digital Personal Data Protection Bill, 2023 (DPDP Bill) [2] and [6], the framework has

been simplified with just the three elements of “notice” and “consent” and “fiduciary duties”, and adds no specific exception with regards to automated decision making and/or human intervention.

4.2 Analysis of Indirect Safeguards under the Act and the 2025 Rules

While the Digital Personal Data Protection Act, 2023 does not expressly refer to automated decision-making in its part on substantive rights, there are a few provisions that indirectly govern the processing of personal data with the use of algorithms:

1. **Definition of Processing (Section 2(x)):** Processing is defined as a "wholly or partly automated operation or series of operations carried out on personal data that involve the use of a digital system or a number of such systems" [2]. Thus, as long as a digital personal data, whether it is ingested, analyzed, or produced, is used by an artificial intelligence model, the obligations of the Act are in effect.
2. **Notice and Purpose Limitation (Sections 4, 5, and 6):** A Data Fiduciary can process personal data only for a lawful purpose if it obtains free, specific, informed, unconditional and unambiguous consent that is preceded by an itemized notice [2]. Rule 3 of the Digital Personal Data Protection Rules, 2025 requires fiduciaries to give notice of the purpose of the processing; however, there is no explicit obligation to disclose the presence of automated decision-making or the algorithmic logic behind it in Section 5 of the Act or Rule 3 of the Digital Personal Data Protection Rules, 2025. [2], [3].
3. **Duty of Data Accuracy in Decision-Making (Section 8(3)):** Section 8(3) is the most obvious connection to automated decision-making. It requires that the Data Fiduciary ensure that the personal data is complete, accurate and consistent when processed by the Data Fiduciary and is likely to be used to make a decision, which affects the Data Principal [2]. Although good, Section 8(3) only deals with input data cleanliness, not procedural fairness. An algorithm may even generate a strongly discriminatory or random result when it receives utterly accurate input data.
4. **Significant Data Fiduciaries and Algorithmic Due Diligence (Section 10 and Rule 13):** Section 10(2) requires SDFs to appoint a Data Protection Officer, hire an independent data auditor, and undertake periodic Data Protection Impact Assessments [2]. Importantly, Rule 13(3) of the Digital Personal Data Protection Rules, 2025 places an obligation on SDFs to exercise due diligence to ensure that technical measures, such as algorithmic software used by SDFs for processing personal data, do not present a risk to the rights of the Data Principals [3]. But this duty applies only to the Significant Data Fiduciaries that the Central Government notifies, and does not provide for an enforceable individual right to human audit.
5. **Rights of Data Principals (Sections 11 to 14 and Rule 14):** Under Chapter III [2] Data Principals have the right to access information about processed data (Section 11), the right of correction and erasure (Section 12), the right to grievance redressal (Section 13) and the right to nominate (Section 14). With regard to action and/or omission of the Data Fiduciary in connection with the exercise of its obligations, Section 13 makes grievance redressal mechanisms easily accessible for the Data Principal. But the Act does not grant the Data Principal the right to rely on the Act itself to uphold any responsibility to provide human interaction or to explain the algorithm's reasoning if the decision is made merely by a machine [11].

4.3 Broad State Exemptions under Section 17

This vulnerability of individuals has been further aggravated by Section 17(2)(a) of the Digital Personal Data Protection Act, 2023, which provides a power to the Central Government to exempt any instrumen-

tality of the State from the application of the Act in the interests of sovereignty, integrity, security of the State, friendly relations with foreign states, maintenance of public order, or preventing incitement to any cognizable offence [2]. Besides, Section 7(b) allows for processing of personal data without consent for the provision of subsidies, benefits, services, certificates, licenses or permits [2]. Indian welfare administration is increasingly using automated eligibility verification and facial recognition authentication – and the lack of consent in processing combined with broad exemptions for welfare executives puts citizens in danger of being excluded without any legal means [5], [6].

5. Constitutional Imperatives: Privacy, Dignity, and Procedural Fairness

The principle of Indian constitutional law is that statutory silence does not preclude fundamental rights. In Justice K. S. Puttaswamy (Retd.) and Another v. Union of India and Others (2017), Justice D. Y. Chandrachud stressed that informational privacy is about ensuring freedom of the person over personal data and preventing the state and other actors from having unlimited access and authority over an individual's information through profiling and surveillance [1]. Justice Sanjay Kishan Kaul also pointed out that business and governmental use of unchecked profiling may have an indirect impact on the choices made by humans and thus limit individual rights [1].

Furthermore, the Constitution of India, Article 14 & Article 21 are directly implicated in purely automated decision making without human intervention. In settled administration and constitutional law, any measure of state action or quasi-public function that impacts civil rights will be subject to the principles of natural justice, including the right to be heard and the obligation to issue a reasoned order. Maneka Gandhi v. Union of India (1978) is a landmark decision of the Supreme Court of India which confirmed that the procedure prescribed by law under the right to life (Article 21) must be fair, just and reasonable, and not arbitrary, fanciful or oppressive [13]. Opaque algorithmic decision that deems a citizen unfit to have a livelihood, financial credit or social security benefits without stating any intelligible reason or providing any opportunity to present mitigating facts before any human adjudicator is a violation of principles of non-arbitrariness under Article 14 and of procedural due process under Article 21.

6. Comparative Legal Analysis: India, the European Union GDPR, and the EU AI Act

Comparative evaluation shows the size of the protection gap if the protection provided by the Digital Personal Data Protection Act, 2023 is compared with the international standards.

Table 1: Comparative Assessment of Automated Decision-Making and Human Intervention Safeguards

Legal Parameter	India (DPDP Act, 2023 & Rules, 2025)	European Union (GDPR, 2016)	European Union (AI Act, 2024)
Explicit Right Against Solely Automated Decisions	Absent; no standalone statutory prohibition or right to object	Expressly guaranteed under Article 22(1) for decisions with legal or significant effects	Reinforced for high-risk AI systems across employment, credit, and public services

Right to Human Intervention	Not mandated as an enforceable Data Principal right	Mandatory safeguard under Article 22(3) when automated processing is permitted	Mandatory human oversight design requirement under Article 14
Right to Explanation of Algorithmic Logic	Absent; limited to general notice of data categories and purpose	Meaningful information about logic required under Articles 13(2)(f), 14(2)(g), and 15(1)(h)	Right to explanation of individual decision-making provided under Article 86
Algorithmic Risk and Impact Assessments	Required only for Significant Data Fiduciaries under Section 10 and Rule 13(3)	Mandatory Data Protection Impact Assessment under Article 35(3)(a) for systematic profiling	Mandatory Fundamental Rights Impact Assessment and conformity assessments
Enforcement and Financial Penalties	Up to INR 250 Crore under Schedule to DPDP Act, 2023	Up to EUR 20 Million or 4 percent of global annual turnover under Article 83(5)	Up to EUR 35 Million or 7 percent of global annual turnover under Article 99

The rights of a data subject in relation to automated processing, including profiling, that produces a legal decision in relation to him or her are guaranteed pursuant to the provisions of Article 22(1) of the GDPR [7]. Article 22(3) imposes on the data controller the obligation to take appropriate measures to protect the data subject's rights, freedoms and legitimate interests, including the right to request intervention by humans on the part of the controller, to give expression to his point of view and to challenge the decision, even where such automated decision making is otherwise lawful under Article 22(2) (such as when it is required to enter into a contract or when express consent is given) [7].

In addition to the General Data Protection Regulation, the European Union Artificial Intelligence Act (EU AI Act) 2024/1689, requires compliance with the duty to be able to adequately supervise the systems in the event they fall under the category of high-risk AI systems by natural persons throughout their use [12]. This suggests that Article 14 explicitly calls for human “overseers” to be capable of understanding the capabilities and constraints of the AI system, to be aware of the problem of automation bias, to be able to interpret the information output of the AI system and to be able to decide not to use the system or to dismiss, override and reverse the information output [12]. In contrast, India's approach to the application of Rule 13(3) of the Digital Personal Data Protection Rules, 2025, which only requires Significant Data Fiduciaries to establish that the software using algorithms is not likely to infringe on the rights of Data Principals, is neither universally applicable nor individualised procedural empowerment [3].

7. Critical Evaluation and Recommendations

Under the Digital Personal Data Protection Act, 2023, there is no right to human intervention which puts Indian citizens at risk in several important aspects of socio-economic life. In the digital lending and credit scoring process, a credit algorithm will reject a loan application without providing any information either about whether the algorithmic error or proxy discrimination resulted in the rejection of a loan application or not. Platform-based gig job or corporate recruitment, automated performance

management algorithms, and resume-screening algorithms frequently discriminate or fire workers without human appeal. Failure of automated deduplication and biometric authentication can result in marginalised citizens being deprived of food rations and pensions in public welfare delivery.

For India's data protection regime to align its measures with the constitutional protections and international best practices and not inhibit new and emerging technologies, the next concrete steps are recommended:

1. **Statutory Amendment to Incorporate Algorithmic Rights:** Parliament should consider statutory amendment to Incorporate Algorithmic Rights in the Digital Personal Data Protection Act, 2023 by introducing a dedicated provision (proposed Section 13A) for Every Data Principal, to have the right to not be subjected to a decision based solely on automated processing that has a legal or similarly significant effect, and to also have the right to request human intervention along with providing additional context and challenging the decision.
2. **Expansion of Notice Requirements under Rule 3 of Digital Personal Data Protection Rules 2025:** The Central Government should extend notice requirements in Rule 3 of Digital Personal Data Protection Rules, 2025 to provide Data Principal, in clear and plain language, with information about the automated processing and its consequences, which is used when personal data is processed for the purpose of automated profiling or automated decision making.
3. **Making Meaningful Human Review Standards actionable:** The Data Protection Board of India should enact authoritative regulations which stipulate that human review must be substantive and not nominal. The reviewing officers should have domain competence, access to the underlying data and decision weights, and complete authority to defy the algorithmic recommendations.
4. **Broadening Algorithmic Due Diligence Beyond Significant Data Fiduciaries:** The algorithmic verification duty under Rule 13(3) of the Digital Personal Data Protection Rules, 2025 should apply to all Data Fiduciaries that use high impact automated decision-making processes, not just those with significant numbers of users, in sectors including banking, insurance, healthcare, employment and education.
5. **Narrowing State Exemptions for Automated Welfare Decisions:** There is need to clarify that duties of data accuracy, reasonable explanation and human grievance redressal apply to state instrumentalities that use automated systems in the delivery of public services and in determining eligibility for welfare benefits, in section 17 of the Digital Personal Data Protection Act, 2023.

8. Conclusion

The Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 have been a stepping stone in the digital governance framework in India [2], [3]. But the statutory framework does not provide a clear distinction between formal data compliance and substantive individual autonomy, because of its lack of both an explicit right against solely automated decision-making and the requirement for meaningful human intervention. [5], [11]. An enforceable procedural right for citizens to question, understand, and appeal machine-generated determinations that impact their rights and livelihoods is a necessary and essential safeguard that can't simply be replaced by the ability to rely on indirect ones, like data accuracy and algorithmic due diligence of Significant Data Fiduciaries. [2], [3]. Therefore, it is crucial to incorporate a substantive right to human intervention into the Indian data protection framework to safeguard human dignity, constitutional due process, and hold AI systems accountable to human action.

References

1. Supreme Court of India, "Justice K. S. Puttaswamy (Retd.) and Another v. Union of India and Others," Supreme Court Cases, vol. 10, pp. 1-721, Sep. 2018. [Online]. Available: https://indiankanoon.org/doc/127517806/
2. Ministry of Law and Justice, Government of India, "The Digital Personal Data Protection Act, 2023 (No. 22 of 2023)," The Gazette of India, pp. 1–21, Aug. 2023. [Online]. Available: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
3. Ministry of Electronics and Information Technology, Government of India, "Digital Personal Data Protection Rules, 2025," G.S.R. 846(E), The Gazette of India, Extraordinary, Nov. 13, 2025. [Online]. Available: https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf
4. Committee of Experts under the Chairmanship of Justice B. N. Srikrishna, "A free and fair digital economy: Protecting privacy, empowering Indians," Ministry of Electronics and Information Technology, Jul. 2018, pp. 1–213. [Online]. Available: https://prsindia.org/files/bills_acts/bills_parliament/2019/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill,%202018_0.pdf
5. D. Mehta and A. Bhandari, "Data privacy in India: A critical analysis of the Digital Personal Data Protection Act, 2023," Indian J. Integr. Res. Law, vol. 6, no. 2, pp. 972–977, 2026. [Online]. Available: https://ijirl.com/wp-content/uploads/2026/04/61.-DATA-PRIVACY-IN-INDIA-A-CRITICAL-ANALYSIS-OF-THE-DIGITAL-PERSONAL-DATA-PROTECTION-ACT-2023.pdf
6. PRS Legislative Research, "The Digital Personal Data Protection Bill, 2023: Legislative brief," Institute for Policy Research Studies, Aug. 2023, pp. 1–6. [Online]. Available: https://prsindia.org/billtrack/prs-products/prs-legislative-brief-4181
7. European Parliament and Council of the European Union, "Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)," Official Journal of the European Union, vol. L 119, pp. 1–88, May 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj
8. S. Wachter, B. Mittelstadt, and L. Floridi, "Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation," Int. Data Privacy Law, vol. 7, no. 2, pp. 76–99, May 2017. [Online]. Available: https://ora.ox.ac.uk/objects/uuid:6c90bb41-093c-417b-852a-7716054e44bb
9. L. Edwards and M. Veale, "Enslaving the algorithm: From a 'right to an explanation' to a 'right to better decisions'?," IEEE Security & Privacy, vol. 16, no. 3, pp. 46–54, May/Jun. 2018, doi: 10.1109/MSP.2018.2701152.
10. Lok Sabha Secretariat, Parliament of India, "The Personal Data Protection Bill, 2019 (Bill No. 373 of 2019)," PRS Legislative Research, Dec. 2019, pp. 1–62. [Online]. Available: https://prsindia.org/files/bills_acts/bills_parliament/2019/Personal%20Data%20Protection%20Bill,%202019.pdf
11. T. and D. S. Srivastava, "Data anonymisation, the right to explanation, and the architecture of accountability under the Digital Personal Data Protection Act," HILSR Law Rev., vol. 1, pp. 91–105, 2025. [Online]. Available:

https://www.jamiahamdard.ac.in/uploads/files/6__Data_Anonymisation,_The_Right_to_Explanation,_and_The_Architecture_of_Accountability_Under_the_Digital_Personal_Data_Protection_Act_.pdf
12. European Parliament and Council of the European Union, "Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)," Official Journal of the European Union, pp. 1–144, Jul. 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/1689/oj
13. Supreme Court of India, "Maneka Gandhi v. Union of India," Supreme Court Cases, vol. 1, p. 248, 1978.