AUTOMATED DECISION-MAKING AND ALGORITHMIC ACCOUNTABILITY: AN EXAMINATION OF REGULATORY GAPS IN INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Rajasri RV, B.Com. LL.B. (Hons.), School of Law, Sastra University

ABSTRACT

India's Digital Personal Data Protection Act, 2023 (DPDPA) is the country's first major data protection law. But as algorithms increasingly decide important things in people's lives like who gets a loan, who gets hired, or who qualifies for welfare, the Act says almost nothing about how these automated decisions should be regulated. This paper looks at that gap. The paper, therefore, analyses the DPDP Act and DPDP Rules, 2025, against the relevant provisions of the EU's GDPR and AI Act to understand how each frameworks deals with automated decision-making, explanation rights and algorithmic audits. Unlike the EU's GDPR, which gives people the right to contest automated decisions and get a human to review them, the DPDPA has no such protection. It doesn't even define terms like "automated decision-making" or "profiling" anywhere in the statute. The paper also examines the Act's only audit mechanism, a narrow, compliance-focused requirement that applies to a small category of government-notified entities and reports only to the regulator, not the public. The problem is worse for algorithms used by the government itself, since the Act allows broad exemptions for state agencies, even in high-stakes areas like policing and welfare distribution. Through this comparative analysis of the DPDP Act against the GDPR and the EU AI Act, this paper argues that India needs clearer rules on automated decision-making, stronger and more independent audits, and real transparency for people affected by algorithmic decisions.

Keywords: DPDP Act, Automated Decision-Making, Algorithmic Audit, Data Protection, Right to Explanation, EU's GDPR.

CHAPTER I – INTRODUCTION

1.1 Background of the Study

Decisions on credit, recruitment and welfare eligibility are increasingly produced or shaped by automated systems that process personal data at scale. Data protection statutes have become the main legal instrument for regulating how such systems treat individuals. India's Digital Personal Data Protection Act, 2023 (DPDP Act) is the country's first comprehensive statute of this kind.[1] The Act contains no express regime for automated decision-making. Its text defines "automated" as a digital process operating automatically on instructions, and defines "processing" as a wholly or partly automated operation on digital personal data.[2] It does not define "automated decision-making" or "profiling", and the rights it grants to a Data Principal are confined to access, correction and erasure, grievance redressal and nomination.

The enabling Rules, notified on 13 November 2025, bring the framework closer to operation. However, rules 3, 5 to 16, 22 and 23 commence only eighteen months after publication.[3] For the largest entities, the closest analogue to an algorithmic safeguard is the regime for Significant Data Fiduciaries: section 10 requires periodic impact assessments and audits, and rule 13(3) requires due diligence that algorithmic software is not likely to pose a risk to Data Principals' rights.

The European Union offers a contrasting model. Article 22(1) of the General Data Protection Regulation (GDPR) gives a data subject the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal or similarly significant effects. Scholarly commentary cautions against treating even this as a settled right to explanation. Wachter, Mittelstadt and Floridi argue that the GDPR's text supports a more limited right to be informed, not an enforceable right to an explanation of individual decisions.[4] The EU Artificial Intelligence Act adds product-style, risk-based obligations for high-risk systems, with Annex

[1] Digital Personal Data Protection Act, 2023, No. 22 of 2023, INDIA CODE (India), the Gazette text at https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf.
[2] DPDP Act § 2(b), (x).
[3] Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), r. 1(4) (Nov. 13, 2025) (India), https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf
[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), art. 22(1), 2016 O.J. (L 119) 1, https://eurlex.europa.eu/eli/reg/2016/679/oj/eng.

III covering uses such as employment and creditworthiness assessment.[5]

According to law-firm commentary, a 2026 amendment postponed the application date for Annex III systems to 2 December 2027.[6]

1.2 Significance of the Study

The study matters for three reasons. First, it concerns a constitutional interest. In *Puttaswamy*, a nine-judge bench held that privacy is a fundamental right under the Constitution, protected within Article 21 and Part III generally.[7] Privacy so understood bears on how personal data is converted into decisions about individuals, and not only on how it is collected or stored. Any State-authored restriction on that right must satisfy the Court's tests of legality, legitimate aim and proportionality.[8]

Second, the gap is practical. A person refused a loan, screened out of a recruitment process or excluded from a welfare scheme by an automated system currently finds no statutory right in the DPDP Act to demand reconsideration by a human or an account of the decision's basis. The accuracy duty in section 8(3) addresses the quality of the input data, not the fairness of the decision.

Third, the timing is favourable to reform. Core obligations are not yet operative, no Data Protection Board practice has accumulated, and the Rules remain amenable to supplementation. Analysis conducted now can therefore inform rule-making and guidance, not merely critique settled enforcement.

1.3 Statement of the Research Problem

The DPDP Act regulates the processing of digital personal data. It does not regulate the manner

---

[5] Sandra Wachter, Brent Mittelstadt & Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7 INT'L DATA PRIVACY L. 76 (2017), https://doi.org/10.1093/idpl/ipx005.

[6] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Act), art. 6, annex III, 2024 O.J. (L 2024/1689), https://eurlex.europa.eu/eli/reg/2024/1689/oj/eng.

[7] *EU AI Act Update: Digital Omnibus Finalizes 8 Compliance Changes*, ORRICK (July 2026), https://www.orrick.com/en/Insights/2026/07/EU-AI-Act-Update-Digital-Omnibus-Finalizes-8-ComplianceChanges

[8] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India), https://indiankanoon.org/doc/91938676/; *see also Fundamental Right to Privacy*, SUPREME COURT OBSERVER, https://www.scobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacy-case-background/

in which that processing is converted into consequential decisions, or how affected individuals may understand and contest them. The safeguards that bear most closely on the problem are indirect and uneven in reach. Section 8(3) is addressed to the completeness, accuracy and consistency of data used in a decision. Section 10 and rule 13 impose impactassessment, audit and algorithmic due-diligence duties only on notified Significant Data Fiduciaries, and the audit report is furnished to the Data Protection Board. Rule 13(3), as worded, concerns technical measures used for hosting, display, publishing, transmission, storage, updating or sharing of personal data, and does not in terms address decisions about individuals. Section 17 further permits wide exemptions for State processing.

The research problem is accordingly twofold. The doctrinal problem is to establish precisely what the Indian framework provides and omits in respect of automated decisionmaking. The normative problem is whether that framework, read with the constitutional guarantee of privacy and measured against the EU's GDPR and AI Act, affords adequate accountability to persons affected by algorithmic decisions.

1.4 Research Objectives

1. To identify what the DPDP Act and the DPDP Rules, 2025 provide, and omit, on automated decision-making, profiling, explanation, human review and algorithmic audit.

2. To evaluate whether section 8(3), section 10 and rule 13 operate as adequate indirect safeguards.

3. To assess the effect of sections 7 and 17 on the accountability of State-operated algorithmic systems.

4. To compare the Indian position with Article 22 GDPR and the risk-based obligations of the EU AI Act.

5. To test the Indian framework against the constitutional standard in *Puttaswamy*.

6. To propose a legislative and regulatory framework for algorithmic accountability in India.

1.5 Research Questions

1. To what extent does the DPDP framework regulate automated decision-making and algorithmic accountability?

2. Does that framework adequately protect individuals affected by consequential automated decisions, in the private and public sectors alike?

3. How do the GDPR and the EU AI Act address automated decision-making, transparency and human intervention, and where does India diverge?

4. Are the audit and impact-assessment mechanisms under section 10 and rule 13 sufficient to address algorithmic risk?

5. Does the exemption architecture of section 17 satisfy the constitutional requirement of proportionality when applied to State algorithmic systems?

6. What reforms are necessary to establish effective algorithmic accountability in India?

1.6 Scope of the Study

The study covers the DPDP Act and the DPDP Rules, 2025, read with Article 21 of the Constitution and *Puttaswamy*. The Information Technology Act, 2000 is considered only where it bears on the argument; the DPDP Act itself provides for the omission of section 43A of that Act.[9] The comparative element is confined to Article 22 and the related transparency provisions of the GDPR, and to the high-risk regime of the EU AI Act as amended in 2026.[10] Case studies from recruitment, credit, welfare, facial recognition and government decision-making illustrate how the identified gaps may operate in practice.

1.7 Limitations of the Study

Several limits qualify the conclusions. First, the Rules were notified on 13 November 2025, and rules 3, 5 to 16, 22 and 23 commence only eighteen months after publication.[11] No Data Protection Board decisions or enforcement practice exist, so the assessment of practical effect

[9] DPDP Act, *supra* note 1, § 44(2)(a).
[10] GDPR, *supra* note 7, art. 22; AI Act, *supra* note 9; *EU AI Act Update*, *supra* note 10.
[11] DPDP Rules, *supra* note 5, r. 1(4).

is prospective. Second, the application dates of the EU AI Act's high-risk provisions have been revised, and this paper relies on secondary commentary for the amendment pending verification of the primary instrument.[12] Third, the comparison is confined to the EU and does not extend to other jurisdictions. Fourth, sectoral regulation, for example by financial or telecommunications regulators, is outside the scope of detailed examination. Fifth, doctrinal analysis cannot measure outcomes empirically, and no technical audit of any algorithmic system is undertaken.

LITERATURE REVIEW

Scholarship on automated decision-making and algorithmic accountability is largely European, and most of it was written around the GDPR and, later, the draft EU AI Act. The sources reviewed below are peer-reviewed. Taken together, they supply the analytical vocabulary for assessing the Indian framework, but none addresses it. What they say is scholarly argument. It is not law, and the discussion that follows treats it accordingly.

The explanation debate

The most cited exchange concerns whether the GDPR confers a "right to explanation". Wachter, Mittelstadt and Floridi argue that it does not. In their reading, the GDPR gives data subjects a more limited right to be informed under Articles 13 to 15 about the logic involved and the significance of automated decision-making. They also contend that Article 22 is ambiguous and narrow in scope, which weakens the protection it appears to offer.[13] Selbst and Powles respond that a return to the text supports a different conclusion. In their view, Articles 13 to 15 entitle a person to "meaningful information" about the logic involved, and this is in substance a right to explanation that should be read functionally, so that it enables the data subject to exercise other rights.[14] Edwards and Veale take a more sceptical position on remedies. They argue that explanation rights are triggered only in restrictive circumstances, that machine-learning explanations rarely match what the law's formulation requires, and that a search for such a right may produce a "transparency fallacy". They point instead to impact assessments, privacy by

[12] *EU AI Act Update*, *supra* note 10.
[13] Wachter, Mittelstadt & Floridi, *supra* note 8.
[14] Andrew D. Selbst & Julia Powles, *Meaningful Information and the Right to Explanation*, 7 INT'L DATA PRIVACY L. 233 (2017), https://papers.ssrn.com/abstract=3039125; *see also* https://escholarship.org/uc/item/9cz6v3zs.

design and the rights of erasure and portability as possible sources of accountability.[15]

These three works matter for India because they show that the existence of an explanation right turns on statutory text. Even a provision as developed as the GDPR's invites dispute. The DPDP Act supplies a weaker textual basis than the GDPR. Section 11(1) entitles a Data Principal to a summary of the personal data processed and the processing activities, and to the identities of other Data Fiduciaries and Processors with whom the data has been shared.[16] Nothing in it concerns the logic of a decision. None of the three works considers a statute of this kind, and their debate presupposes at least some textual hook for explanation. The question for the Indian context is therefore prior to theirs: whether any such hook exists at all.

Individual rights and systemic accountability

Kaminski offers the most useful frame for evaluating the Indian design. Her "binary governance" thesis holds that individual due-process rights and systemic, collaborative regulation address different concerns and that neither suffices alone. Individual rights respond to dignitary and justificatory interests, while systemic mechanisms respond to harms visible only in aggregate. She also argues that the systemic layer fails without public- and stakeholderfacing accountability.[17] Her analysis is directed at the GDPR. Applied to India, the frame yields an observation that this paper develops: the DPDP framework has a thin systemic layer in the

Significant Data Fiduciary duties of section 10 and rule 13, with audit findings reported to the Board, and no individual layer concerning automated decisions.[18] Kaminski does not address State exemptions of the kind found in section 17, and this paper extends her frame to them.

The EU AI Act as a model

Veale and Zuiderveen Borgesius analyse the Commission's 2021 draft of the AI Act. They regard its differentiated, risk-based rules as sensible, but they argue that its reliance on product-safety techniques may leave some provisions ineffective for protecting fundamental rights, and

[15] Lilian Edwards & Michael Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, 16 DUKE L. & TECH. REV. 18 (2017), https://scholarship.law.duke.edu/dltr/vol16/iss1/2.
[16] DPDP Act, *supra* note 1, § 11(1).
[17] Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529 (2019), https://scholar.law.colorado.edu/articles/1265.
[18] DPDP Act, *supra* note 1, § 10(2); DPDP Rules, *supra* note 5, r. 13(1)–(2).

they raise concerns about enforcement.[19] The article is valuable as a caution against importing the AI Act uncritically. Its limits are two. It examines the draft, not the adopted Regulation, and the high-risk timetable has since been revised. It also does not consider whether a jurisdiction lacking a general AI statute could rely on data protection law alone.

The Indian context

Marda's article, which predates the DPDP Act, examines Indian AI policy through the limits of data-driven decision-making, and it is one of the few peer-reviewed works in this field to focus on India.[20] It frames the problem as one of fundamental rights and policy design, which is consistent with this paper's approach. Because it predates both the Act and the Rules, it cannot address the statutory text analysed here.

The research gap

Four gaps emerge. First, the explanation debate concerns the GDPR, and the equivalent question for a statute without an Article 22 analogue has not been examined in the sources reviewed. Second, the individual-rights and systemic-accountability frame has not been applied to the DPDP Act and Rules together. Third, the interaction between the section 17 exemptions and the accountability of State algorithmic systems falls outside the European scholarship, which does not face such broad exemptions. Fourth, Indian scholarship in these sources predates the Act and the 2025 Rules.

This paper addresses those gaps through a close reading of the Act and Rules, tested against the GDPR and the AI Act and the constitutional standard in *Puttaswamy*. It is limited to the sources identified and does not claim to have exhausted the Indian literature published since 2023.

CHAPTER II – LEGAL AND CONCEPTUAL FRAMEWORK

Research Methodology

The study is doctrinal, comparative and analytical. Primary sources comprise the DPDP Act

[19] Michael Veale & Frederik Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act*, 22 COMPUT. L. REV. INT'L 97 (2021), https://doi.org/10.9785/cri-2021-220402.
[20] Vidushi Marda, *Artificial Intelligence Policy in India: A Framework for Engaging the Limits of Data-Driven Decision-Making*, PHIL. TRANSACTIONS ROYAL SOC'Y A (2018) (theme issue on governing artificial intelligence), table of contents at https://www.jstor.org/stable/e26601830.

and Rules (read from the Gazette and India Code texts), the Constitution, the Information

Technology Act, 2000, *Puttaswamy*, Regulation (EU) 2016/679 and Regulation (EU) 2024/1689 (from EUR-Lex). Secondary sources comprise peer-reviewed articles on automated decision-making and explainability, institutional reports and reputable news reporting for the case studies.

For each issue, the analysis proceeds from the statutory text to the identified gap, its practical effect, the comparative position, and then to the researcher's finding and a possible reform. Throughout, the paper distinguishes what a statute provides, what courts have held, what government has stated, what scholars argue, and what the researcher concludes. Academic argument and news reports are not treated as legal authority, and proposed reforms are not presented as existing law.

2.1 Meaning and Nature of Automated Decision-Making

No Indian statute defines automated decision-making. The DPDP Act defines only the narrower term "automated", meaning a digital process capable of operating automatically on instructions.[21] For the purposes of this paper, the researcher adopts a working definition: an automated decision is a determination about an identifiable individual that is produced by a computational process with no meaningful human evaluation of the outcome. This is a working definition and not a statutory one. It follows the structure of Article 22(1) GDPR, which turns on decisions "based solely on automated processing" that produce legal or similarly significant effects. Two categories should be distinguished. In solely automated decisions, the system's output is the decision. In decision-support, a human nominally decides but the output heavily conditions the result. The distinction matters because a rule confined to the first category can be avoided by inserting a formal human step, a weakness taken up in Chapter IV.

2.2 Constitutional Right to Privacy in India

In *Puttaswamy*, a nine-judge bench held that privacy is a fundamental right protected within Article 21 and Part III of the Constitution.[22] In his plurality opinion, Chandrachud J. grounded

[21] DPDP Act, note 1, § 2(b); GDPR, *supra* note 7, art. 22(1).
[22] INDIA CONST. art. 21; *Puttaswamy*, (2017) 10 SCC 1, *supra* note 11.

privacy in autonomy and dignity, as summarised in commentary.[23] The significance for this paper is twofold. Algorithmic decisions that affect liberty, livelihood or access to public benefits engage dignity directly. The right is also enforceable against the State, which is both a major user of automated systems and, through section 17, the principal beneficiary of exemptions from the DPDP Act.

2.3 *Puttaswamy* and Informational Privacy

Puttaswamy treats informational privacy as a facet of the right to privacy. According to commentary on the plurality opinion, any interference must satisfy legality, a legitimate aim and proportionality. *Puttaswamy* does not itself address algorithmic decision-making. The constitutional argument developed in later chapters is therefore the researcher's inference from the decision's principles and is not an existing holding. The inference is that State exemptions from data protection obligations, where applied to automated systems that decide on benefits or policing, must be capable of justification under the three-fold test.

2.4 Existing Indian Legal Framework

India has no dedicated statute on automated decision-making or AI. The relevant framework consists of three layers. The first is constitutional (Articles 14 and 21), which supplies the standards against which State action is tested. The second is statutory data protection. The DPDP Act has displaced the earlier regime under the Information Technology Act, 2000, since it omits section 43A of that Act.[24] The third is policy. On 5 November 2025, MeitY released the India AI Governance Guidelines. According to law-firm commentary on those Guidelines, they decline to propose a standalone AI statute and rely instead on existing laws, including data protection, supplemented by targeted amendments where needed.[25] These are statements of government policy, and they do not create enforceable rights.

---

[23] Hugh Tomlinson, *Case Law, India: Puttaswamy v Union of India, Supreme Court Recognises a Constitutional Right to Privacy in a Landmark Judgment*, INFORRM (Sept. 4, 2017), https://inforrm.org/2017/09/04/case-lawindia-puttaswamy-v-union-of-india-supreme-court-recognises-a-constitutional-right-to-privacy-in-a-landmarkjudgment-hugh-tomlinson-qc/

[24] DPDP Act, note 1, § 44(2)(a).

[25] Ministry of Electronics & Information Technology, *India AI Governance Guidelines* (Nov. 5, 2025); *see MeitY Releases Guidelines on AI Governance – The Way Ahead and Roadmap for AI Use in India*, AZB & PARTNERS (Nov. 13, 2025), https://www.azbpartners.com/bank/meity-releases-guidelines-on-ai-governance-the-wayahead-and-roadmap-for-ai-use-in-india/

2.5 DPDP ACT, 2023 AND REGULATORY GAPS

Overview of the DPDP Act, 2023

The DPDP Act applies to digital personal data processed in India, and to processing outside India connected with offering goods or services to persons in India.[26] It operates through Data Fiduciaries, who determine the purpose and means of processing, and Data Principals, the individuals concerned. Its enforcement body is the Data Protection Board. The Act comes into force in stages by notification, under section 1(2).

Data Principals and Their Rights

The Act confers four rights: access to information about personal data (section 11), correction, completion, updating and erasure (section 12), grievance redressal (section 13) and nomination (section 14). Section 11(1) entitles a Data Principal to a summary of the personal data processed and the processing activities, and to the identities of other Data Fiduciaries and Processors with whom data has been shared. None of the four concerns how a decision about the individual was reached.

A structural feature narrows these rights further. Sections 11(1) and 12(1) are framed by reference to a Data Fiduciary "to whom she has previously given consent", including consent referred to in section 7(a). The researcher's reading is that the access and correction rights are tied to consent-based processing. Processing on other legitimate uses under section 7, including State benefits under section 7(b)(ii), statutory functions under section 7(c) and employment under section 7(i), may therefore fall outside them. This is an interpretive reading of the text, not a holding, and it awaits authoritative interpretation. If correct, it affects precisely the contexts in which consequential automated decisions are made, namely State benefit allocation and workplace decisions.

Data Fiduciaries

A Data Fiduciary remains responsible for compliance, including for processing carried out by its Processors. Two general duties bear on automated decisions. Section 8(3) requires completeness, accuracy and consistency of personal data likely to be used for a decision

[26] DPDP Act, note 1, § 3.

affecting the Data Principal. Section 8(4) requires "appropriate technical and organisational measures" to ensure effective observance of the Act. Section 8(3) is directed at data quality. A system trained on accurate but unrepresentative data, or one that weights accurate data unfairly, does not breach it on its terms. This is the researcher's finding.

Significant Data Fiduciaries

The Central Government may notify a Data Fiduciary or class as a Significant Data Fiduciary, assessing factors that include the volume and sensitivity of data and the risk to Data Principals' rights. A notified entity must appoint an India-based Data Protection Officer and an independent data auditor, and must undertake periodic Data Protection Impact Assessments and audits. Section 17(3) allows the Central Government to exempt notified Data Fiduciaries or classes, expressly including startups, from section 10 and from section 8(3). The most demanding accountability provisions are therefore both discretionary in application and removable by notification. A startup deploying a consequential recruitment or credit-scoring tool could be outside them.

Algorithmic Decision-Making under the Act

The Act and Rules refer to decisions in only five places: section 8(3); section 17(2)(b), which exempts research processing where data is not used for a decision specific to a Data Principal; section 17(4), which relaxes section 12(2) where State processing does not involve a decision that affects the Data Principal; rule 13(3); and the accuracy standard in the Second Schedule. These references show that the legislature recognised decision-making as a regulatory category. It used the concept to define exemptions, and it attached no accountability mechanism to it.

Absence of an Express Right against Solely Automated Decisions

No provision permits a Data Principal to object to, contest or seek human reconsideration of an automated decision. Article 22(1) GDPR provides that right in terms for decisions with legal or similarly significant effects. The Indian practical effect is that a refusal of credit or employment by an automated system is lawful or unlawful under the DPDP Act only by reference to general duties such as accuracy, and the affected person has no route to compel review.

Absence and Limitations of a Right to Explanation

The Act supplies no right to be told the logic or main factors of a decision. Rule 14(3) requires

grievance systems to respond within a period not exceeding ninety days, but the grievance right in section 13 is confined to acts or omissions in the performance of obligations or exercise of rights under the Act. A complaint that an automated decision was wrong or unfair does not fall within it unless a specific statutory duty was breached. The researcher finds that explanation is absent as a legal entitlement.

Algorithmic Auditing and Impact Assessment

The Act's only audit and impact-assessment mechanism is section 10(2) read with rule 13. Rule 13(1) requires an annual assessment and audit, and rule 13(2) requires the person conducting it to furnish the Board with a report of "significant observations". Three limits emerge. The mechanism applies only to notified entities. The audit evaluates compliance with the Act and is not directed at the fairness or accuracy of outcomes. And nothing in the text requires publication or disclosure of findings to affected persons.

Rule 13(3) requires a Significant Data Fiduciary to exercise due diligence to verify that technical measures, "including algorithmic software", are not likely to risk Data Principals' rights. Its subject matter, however, is technical measures for hosting, display, publishing, transmission, storage, updating or sharing of personal data. On its wording, it reaches datahandling and platform systems, and it does not on its face extend to decision systems that score or classify individuals. The researcher regards this as the closest Indian approximation to an algorithmic safeguard and as materially narrower than a decision-focused duty.

Government Exemptions

State processing is the least regulated category. Section 7(b) and (c) allow processing for subsidies, benefits and statutory functions without consent. Section 17(1)(c) disapplies most obligations for processing in the interest of preventing, detecting or investigating offences. Section 17(2)(a) permits the Central Government to notify State instrumentalities for complete exemption from the Act on grounds including security of the State and public order. For State benefit processing, rule 5 and the Second Schedule impose standards, including lawful processing, necessity, reasonable efforts at accuracy, intimation to the Data Principal and accountability. These do not include a right to contest or an explanation.

2.6 COMPARATIVE LEGAL ANALYSIS

GDPR Article 22

Article 22(1) gives the data subject the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects or similarly significantly affects them. Article 22(2) disapplies this where the decision is necessary for a contract, authorised by Union or Member State law with suitable safeguards, or based on explicit consent. Where the contract or consent exceptions apply, Article 22(3) still requires the controller to implement at least the right to obtain human intervention, to express a point of view and to contest the decision. Article 22(4) restricts decisions based on special categories of data.

Article 22 has a well-known weakness, which is the word "solely". A formal human step could take a decision outside it. The Court of Justice addressed a version of this in *SCHUFA*. It held that where a credit agency's automated probability value is drawn on decisively by a third party in deciding on a loan, the establishment of the value is itself an automated individual decision within Article 22(1).[27] It supplies a functional test, looking to the determining role of the output, as a counter to circumvention.

Right to Explanation and Transparency

The scholarly dispute reviewed in the Literature Review has been overtaken in part by case law. In *CK v Dun & Bradstreet Austria*, the Court held that, for automated decision-making within Article 22(1), the data subject may require the controller to explain, in a concise, transparent, intelligible and easily accessible form, the procedure and principles actually applied to obtain the result.[28]

Algorithmic Audits and Accountability

Under the AI Act, certain deployers must carry out a fundamental rights impact assessment

[27] Case C-634/21, SCHUFA Holding (Scoring), ECLI:EU:C:2023:957 (Dec. 7, 2023); *see CJEU Rules That a Credit Score Constitutes Automated Decision Making Under the GDPR*, A&O SHEARMAN, https://www.aoshearman.com/en/insights/ao-shearman-on-data/cjeu-rules-that-a-credit-score-constitutesautomated-decision-making-under-the-gdpr (law-firm commentary).

[28] Case C-203/22, CK v. Dun & Bradstreet Austria GmbH, ECLI:EU:C:2025:117, ruling ¶ 1 (Feb. 27, 2025), https://fra.europa.eu/en/node/46254 (reproducing the operative part); *see also* Court of Justice of the European Union, Press Release No. 22/25 (Feb. 27, 2025), https://curia.europa.eu/jcms/upload/docs/application/pdf/2025-02/cp250022en.pdf.

before first use of an Annex III system. These are public bodies, private entities providing public services, and deployers of credit-scoring and certain insurance systems. The assessment complements any GDPR data protection impact assessment.[29] By comparison, rule 13 of the DPDP Rules requires an annual impact assessment and audit by Significant Data Fiduciaries only, with a report of significant observations to the Board. Two qualifications apply to the comparison. The EU regime is not a public-disclosure model either, though registration of high-risk systems in an EU database provides some public-facing transparency. And an impact assessment is not the same as an independent audit of outcomes. The comparative point is narrower: the EU regime extends duties to public-sector deployers and defined private deployers by reference to the use, whereas the Indian regime depends on entity designation.

Lessons for India

First, an Indian provision should be framed around the determining role of the automated output, not only "solely" automated decisions, since *SCHUFA* shows how a narrow trigger invites circumvention. Second, explanation should be defined by function, as in *Dun & Bradstreet*: the procedure and principles actually applied, with a mechanism for resolving trade-secret claims. Third, obligations should be graded by use-case and not only by entity. Fourth, impact assessment should extend to State deployers, the category most insulated under section 17.

2.7 CASE STUDIES AND PRACTICAL IMPLICATIONS

Recruitment: Amazon's Experimental Hiring Tool

According to Reuters, Amazon's machine-learning team began building a tool in 2014 to review résumés and rank candidates. The system penalised résumés containing the word "women's" and downgraded graduates of two all-women's colleges. Amazon's recruiters, the report said, looked at the tool's recommendations but never relied solely on its rankings.

Amazon told Reuters the tool was never used by recruiters to evaluate candidates, and the effort was abandoned.[30] Reuters also quoted critics who observed that it would be very difficult to sue

[29] AI Act, *supra* note 9, art. 27, https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-27 (European Commission AI Act Service Desk); GDPR, *supra* note 7, art. 35.

[30] Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*, REUTERS (Oct. 10, 2018) [VERIFICATION REQUIRED: confirm the Reuters URL; the link you supplied could not be opened and differs in one character from the identifier used in other citations]; *see* wire copy at EURONEWS, https://www.euronews.com/business/2018/10/10/amazon-scraps-secret-ai-recruiting-toolthat-showed-bias-against-women.

over automated hiring, because candidates might never know it was used.

Application of the DPDP Act (researcher's analysis). An Indian applicant who submits a résumé would generally be a Data Principal whose data is processed for a specified purpose under section 7(a) or on consent. The DPDP Act would require notice of the purposes, but nothing requires disclosure that a ranking algorithm is used. Section 8(3) would require that the résumé data be complete and accurate, and the data in a case like Amazon's was not inaccurate. The defect lay in what the model learned from historical hiring patterns. A section 8(3) claim therefore fails on its terms. The employer would be subject to section 10 only if notified as a Significant Data Fiduciary, and section 17(3) permits exemption of classes of fiduciaries, including startups. Under the EU framework, by contrast, employment systems fall within Annex III of the AI Act as high-risk, and Article 22 GDPR would apply to solely automated rejections. *Finding:* the Indian framework gives a rejected applicant no entry point to discover or contest an algorithmic screen.

Welfare: Samagra Vedika and SyRI

Al Jazeera's 2024 investigation, produced with the Pulitzer Center's AI Accountability Network, reported on Samagra Vedika, a system that Telangana uses to cross-match citizen records from multiple government databases to assess eligibility and flag suspected fraud. The investigation described a woman denied food-security benefits after the system conflated her late husband with a car owner of a similar name. Officials were required to check the system's output before approving applications and could depart from it only by recording reasons, but in her case the authorities accepted the algorithm's result. The state IT department refused RTI requests for the source code, citing the vendor's rights over it.[31] An Amnesty International technical explainer published in 2024 examined the entity-resolution method used and raised human-rights concerns.[32] These are investigative and advocacy findings. They are not judicial findings, and the government's position on them is not recorded in the sources reviewed.

Application of the DPDP Act (researcher's analysis). Processing for State benefits falls within

[31] Tapasya, Kumar Sambhav & Divij Joshi, *How an Algorithm Denied Food to Thousands of Poor in India's Telangana*, AL JAZEERA (Jan. 24, 2024), https://www.aljazeera.com/economy/2024/1/24/how-an-algorithmdenied-food-to-thousands-of-poor-in-indias-telangana.

[32] Amnesty International, *Use of Entity Resolution in India: Shining a Light on How New Forms of Automation Can Deny People Access to Welfare* (Apr. 2024), https://www.amnesty.org/en/latest/research/2024/04/entityresolution-in-indias-welfare-digitalization/.

section 7(b). The Telangana facts also show why a "solely automated" threshold is inadequate. The decision was formally taken by a human official, yet the algorithm's output effectively settled it. This is the circumvention risk that *SCHUFA* addresses by looking to the determining role of the output. *Finding:* the Act offers neither a trigger that captures such "human-in-the-loop" deference nor a mechanism that would have exposed the system's error rate.

Facial Recognition and Surveillance: Delhi Police

In RTI replies dated July 2022, obtained by the Internet Freedom Foundation after proceedings before the Central Information Commission, the Delhi Police stated that it treats matches above 80 per cent similarity as positive. Matches below that figure are labelled "false positive" but remain subject to "due verification with other corroborative evidence".[33] The reports carrying these disclosures also note that the technology was used in the investigation of the North East Delhi riots. These are the police's own statements as disclosed under RTI, and the characterisations of their adequacy are advocacy commentary. *Application of the DPDP Act (researcher's analysis).* Processing for the prevention, detection or investigation of offences falls within section 17(1)(c), which disapplies the Data Principal's rights and most Data Fiduciary obligations. Where the police are notified under section 17(2)(a), the Act would not apply at all. A person flagged by such a system would have no statutory right to be told, to seek correction or to contest. Whether the arrangement meets the legality, legitimate-aim and proportionality tests derived from *Puttaswamy* is a constitutional question that no authority in the sources reviewed has resolved, and this paper expresses no conclusion on it. *Finding:* section 17 places this category of algorithmic State action largely outside the data protection framework, so that accountability depends on constitutional litigation and RTI requests.

CHAPTER III – CONCLUSION

This paper asked whether India's data protection framework, as it stands in the DPDP Act, 2023 and the DPDP Rules, 2025, is adequate to secure accountability for decisions made wholly or partly by algorithms. The answer on the statutory text is that it is not. The Act regulates the

[33] *Delhi Police's Claims That FRT Is Accurate with a 80% Match Are 100% Scary*, INTERNET FREEDOM FOUNDATION, https://internetfreedom.in/delhi-polices-frt-use-is-80-accurate-and-100-scary/ (advocacy organisation; reproducing Delhi Police RTI replies); *80% Accuracy in Facial Recognition Database Is a Positive Match for Delhi Police: Report*, DECCAN HERALD, https://www.deccanherald.com/amp/story/india/80accuracy-in-facial-recognition-database-is-a-positive-match-for-delhi-police-report-1136806.html

processing of personal data, and it does recognise decisions as a category through the accuracy duty in section 8(3). It attaches no right, duty or oversight mechanism to automated decisions as such. A person refused credit, employment or a welfare benefit by an automated system has no statutory entitlement to human review, to an account of the decision's basis, or to have the system independently tested.

The broader answer to the paper's central question is that a technology-neutral data protection statute can be a foundation for algorithmic accountability but cannot be the whole structure. Individual rights of review and explanation, systemic assessment and audit, and public-sector oversight have to be built on that foundation. The reforms proposed in Chapter VI are designed to be proportionate. They are triggered by consequential decisions, and they keep proprietary material confidential to the regulator. Because the substantive provisions have not yet commenced, there is still room to give the framework operative content through rules, Board guidance and legislative amendment before enforcement practice hardens around the present text.

CHAPTER IV – FINDINGS, RECOMMENDATIONS AND FUTURE DIRECTIONS

4.1 Major Findings

First, the DPDP Act and Rules contain no definition of automated decision-making or profiling and no right against, or to contest, a solely or predominantly automated decision. The only textual references to "decisions" serve the accuracy duty in section 8(3) and the calibration of exemptions. Second, explanation is absent as a legal entitlement. Section 11(1) yields a summary of data and its sharing, and the grievance route in section 13 is confined to breaches of the Act. Third, the audit and impact-assessment machinery in section 10 and rule 13 is entitylimited, compliance-oriented and addressed to the Board. Rule 13(3), on its wording, targets data-handling systems and not decision systems. Fourth, sections 7 and 17 leave State algorithmic systems in welfare and policing largely outside the framework. Fifth, substantial discretion over designation, exemption and Board composition rests with the Central Government.

4.2 Recommendations

The recommendations below are proposals and not existing law. They are ordered by feasibility.

Some can be achieved by amending the Rules, issuing Board guidance or adding to notices, within the Act's rule-making powers. A new substantive right against automated decisions would, in the researcher's view, more securely rest on a statutory amendment, since it is unlikely to fall within the existing rule-making heads. The Act is expressed to operate in addition to other laws, which leaves room for a complementary instrument on high-risk systems.

4.3 Proposed Legal Framework for Automated Decision-Making

The researcher proposes a statutory provision with three elements. First, definitions of "automated decision", "profiling" and "consequential decision", the last meaning a decision with legal or similarly significant effects, including on credit, employment, access to public benefits and liberty. Second, a right not to be subject to a consequential decision where an automated output has a determining role, subject to exceptions for authorised law with safeguards, contractual necessity and explicit consent. A determining-role test is preferable to a "solely automated" test, because *SCHUFA* and the Telangana facts show that a nominal human step can defeat the latter. Third, where an exception applies, mandatory safeguards of human review, an opportunity to be heard and the right to contest.

4.4 Independent Algorithmic Audits

The audit under rule 13 should be extended in two respects for consequential systems: independence, through accredited auditors who are not engaged by the fiduciary for other services, and scope, through outcome-based testing for accuracy and discriminatory effect alongside compliance. Reports should be furnished to the Board in full, and a non-confidential summary should be public. Kaminski's argument that systemic accountability requires some public- or stakeholder-facing element supports publication. Trade-secret concerns should be resolved by confidential disclosure to the Board, in line with the Court of Justice's approach that an authority or court decides the balance.

4.5 Right to Explanation

The right should be defined functionally. An affected person should be able to obtain notice that an automated system was used, the main factors and the procedure and principles applied, in language and form the person can understand. This tracks the Court of Justice's reading of the equivalent GDPR right. An explanation right of this kind is a precondition for contestation,

since a person cannot challenge what they cannot see. It should be accompanied by an extension of the grievance right in section 13 to cover automated decisions.

4.6 Stronger Oversight of Government AI Systems

The exemptions should be narrowed as they apply to algorithmic decisions about individuals. Even where Chapter II rights are disapplied, State bodies should be required to have a statutory basis for the system, to conduct and record a proportionality assessment of the kind *Puttaswamy* requires, and to be subject to independent oversight. Notifications under section 17(2)(a) should be published with reasons. The independence of the Board, whose members the Central Government appoints, should be strengthened, since a Board with real authority over State systems is a precondition for any of the above.

4.7 Future Directions

Five lines of inquiry follow. First, the Board's practice after the substantive provisions commence should be studied to test the textual readings advanced here. Second, empirical research should assess whether audits under rule 13 detect and prevent algorithmic harm. Third, the interaction with sectoral regulators of finance and telecommunications requires separate analysis. Fourth, Indian courts' treatment of algorithmic State action under Articles 14 and 21 should be tracked. Fifth, comparative work should follow the implementation of the EU AI Act and the Court of Justice's developing case law, and widen beyond the EU.

CHAPTER V: REFERENCES

A. Statutes and Rules (India)

Digital Personal Data Protection Act, 2023, No. 22 of 2023, INDIA CODE (India), (Gazette text: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf).

Digital Personal Data Protection Rules, 2025, G.S.R. 846(E) (Nov. 13, 2025) (India), https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf.

INDIA CONST. arts. 14, 21. [VERIFICATION REQUIRED: add an official Constitution link, for example from India Code or the Legislative Department.]

B. Cases

India

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India), https://indiankanoon.org/doc/91938676/.

European Union

Case C-634/21, SCHUFA Holding (Scoring), ECLI:EU:C:2023:957 (CJEU Dec. 7, 2023). [VERIFICATION REQUIRED: official CURIA or EUR-Lex link.]

Case C-203/22, CK v. Dun & Bradstreet Austria GmbH, ECLI:EU:C:2025:117 (CJEU Feb. 27, 2025), https://fra.europa.eu/en/node/46254; Press Release No. 22/25,

https://curia.europa.eu/jcms/upload/docs/application/pdf/2025-02/cp250022en.pdf.

Netherlands

Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:1878 (Neth.), https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878.

C. European Union and International Instruments

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1, https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Act), 2024 O.J. (L 2024/1689), https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng. *Article texts consulted:* art. 27, https://ai-act-servicedesk.ec.europa.eu/en/ai-act/article-27; art. 86, https://ai-act-service-desk.ec.europa.eu/en/aiact/article-86.

OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (as

revised May 3, 2024). [VERIFICATION REQUIRED: official OECD Legal Instruments URL.]

D. Books and Journal Articles (peer-reviewed)

Lilian Edwards & Michael Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, 16 DUKE L. & TECH. REV. 18 (2017),

https://scholarship.law.duke.edu/dltr/vol16/iss1/2.

Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529 (2019), https://scholar.law.colorado.edu/articles/1265.

Naomi Appelman, Ronan Ó Fathaigh & Joris van Hoboken, *Social Welfare, Risk Profiling and Fundamental Rights: The Case of SyRI in the Netherlands*, 12 JIPITEC (issue 4) (2021), https://www.ivir.nl/publicaties/download/jipitec_2021_4.pdf. [VERIFICATION REQUIRED: page range.]

Andrew D. Selbst & Julia Powles, *Meaningful Information and the Right to Explanation*, 7 INT'L DATA PRIVACY L. 233 (2017), https://papers.ssrn.com/abstract=3039125. [VERIFICATION REQUIRED: DOI of the published version.]

Michael Veale & Frederik Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act*, 22 COMPUT. L. REV. INT'L 97 (2021), https://doi.org/10.9785/cri-2021220402.

Sandra Wachter, Brent Mittelstadt & Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7 INT'L DATA PRIVACY L. 76 (2017), https://doi.org/10.1093/idpl/ipx005.

Vidushi Marda, *Artificial Intelligence Policy in India: A Framework for Engaging the Limits of Data-Driven Decision-Making*, PHIL. TRANSACTIONS ROYAL SOC'Y A (2018), issue contents at https://www.jstor.org/stable/e26601830. [VERIFICATION REQUIRED: volume, article number, DOI and direct URL. Drop this entry if it cannot be confirmed.]

E. Official and Institutional Sources

Ministry of Electronics & Information Technology, *India AI Governance Guidelines* (Nov. 5, 2025). [VERIFICATION REQUIRED: link to the primary text on the MeitY or PIB site.]

Amnesty International, *Use of Entity Resolution in India: Shining a Light on How New Forms of Automation Can Deny People Access to Welfare* (Apr. 2024), https://www.amnesty.org/en/latest/research/2024/04/entity-resolution-in-indias-welfaredigitalization/.

F. News Reports and Online Commentary (factual record or orientation only; not legal authority)

Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*,

REUTERS (Oct. 10, 2018). [VERIFICATION REQUIRED: confirm the Reuters URL.] Wire copy: EURONEWS, https://www.euronews.com/business/2018/10/10/amazon-scraps-secretai-recruiting-tool-that-showed-bias-against-women.

Tapasya, Kumar Sambhav & Divij Joshi, *How an Algorithm Denied Food to Thousands of Poor in India's Telangana*, AL JAZEERA (Jan. 24, 2024), https://www.aljazeera.com/economy/2024/1/24/how-an-algorithm-denied-food-to-thousandsof-poor-in-indias-telangana. [VERIFICATION REQUIRED: author line.]

Delhi Police's Claims That FRT Is Accurate with a 80% Match Are 100% Scary, INTERNET FREEDOM FOUNDATION, https://internetfreedom.in/delhi-polices-frt-use-is-80-accurateand-100-scary/ (advocacy organisation).

80% Accuracy in Facial Recognition Database Is a Positive Match for Delhi Police: Report, DECCAN HERALD, https://www.deccanherald.com/amp/story/india/80-accuracy-in-facialrecognition-database-is-a-positive-match-for-delhi-police-report-1136806.html. [VERIFICATION REQUIRED: publication date and original Indian Express article.]

Hugh Tomlinson, *Case Law, India: Puttaswamy v Union of India, Supreme Court Recognises a Constitutional Right to Privacy in a Landmark Judgment*, INFORRM (Sept. 4, 2017), https://inforrm.org/2017/09/04/case-law-india-puttaswamy-v-union-of-india-supreme-courtrecognises-a-constitutional-right-to-privacy-in-a-landmark-judgment-hugh-tomlinson-qc/ (secondary; replace with judgment pin-cites).

Fundamental Right to Privacy, SUPREME COURT OBSERVER, https://www.scobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacycase-background/ (case summary).

MeitY Releases Guidelines on AI Governance – The Way Ahead and Roadmap for AI Use in India, AZB & PARTNERS (Nov. 13, 2025), https://www.azbpartners.com/bank/meityreleases-guidelines-on-ai-governance-the-way-ahead-and-roadmap-for-ai-use-in-india/ (lawfirm commentary).

EU AI Act Update: Digital Omnibus Finalizes 8 Compliance Changes, ORRICK (July 2026), https://www.orrick.com/en/Insights/2026/07/EU-AI-Act-Update-Digital-Omnibus-Finalizes8-Compliance-Changes (law-firm commentary).

CJEU Rules That a Credit Score Constitutes Automated Decision Making Under the GDPR, A&O SHEARMAN, https://www.aoshearman.com/en/insights/ao-shearman-on-data/cjeurules-that-a-credit-score-constitutes-automated-decision-making-under-the-gdpr (law-firm commentary).