INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA).*

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

ALGORITHMIC PRIVACY AND THE DIGITAL PERSONAL DATA PROTECTION ACT 2023: A COMPARATIVE ANALYSIS WITH INTERNATIONAL STANDARDS.

AUTHORED BY - TANMAY SRIVASTAVA & SARBANI DEB

Abstract

Rapid developments in artificial intelligence, big-data analytics, and automated decision-making have converted privacy past traditional informational concerns toward a compound frontier of "algorithmic privacy," encompassing opacity, bias, and machine-driven harms. India's Digital Personal Data Protection Act 2023 (DPDP Act) characterises a landmark answer to evolving data protection encounters, yet its consent-centric, technology-neutral structure offers only incidental precautions against risks arising from profiling, large-scale inference, and fully or partly automated decisions. This paper appraises the DPDP Act as an instrument for prevailing algorithmic privacy, situating it within India's constitutional right to privacy framework and associating it with international data protection regimes, predominantly the EU General Data Protection Regulation (GDPR), the EU AI Act, and selected frameworks from North America and the Asia-Pacific region. The analysis identifies four systemic gaps in the DPDP architecture: weak explicit recognition of automated decision-making harms, absence of an impartial right to explanation or human review, limited guidance on algorithmic impact assessment and auditing, and broad state exemptions that destabilise constitutional proportionality standards. While the DPDP Act converges with global principles of lawfulness, purpose limitation, and accountability, it lags behind leading jurisdictions in operationalizing algorithmic transparency, fairness, and contestability, especially in high-risk AI contexts such as recruitment, credit, insurance, and public sector surveillance. The paper undertakes by proposing a layered reform agenda incorporating AI-specific duties through targeted amendments or rules, enhanced individual rights against consequential automated decisions, and a more independent, expert-driven Data Protection Board equipped to supervise audits and sectoral codes of practice.

Keywords: Digital Personal Data Protection Act, Automated Decision-Making, Informational Privacy, Algorithmic Bias, Comparative Data Protection Law.

ISSN: 2582-6433

Introduction

The digital revolution has fundamentally transformed how personal data is composed, administered, and operated across global economies. Where once privacy concerns centred on the unauthorized revelation of personal information or unfitting surveillance, the contemporary landscape presents far more complex challenges. The proliferation of artificial intelligence systems, machine learning algorithms, and big-data analytics stages has created an entirely new category of privacy risks—what scholars and controllers increasingly term "algorithmic privacy." This concept encompasses beyond the traditional informational privacy paradigm to encompass the impenetrability of algorithmic decision-making processes, the pervasive risks of discriminatory bias embedded within AI systems, the harms arising from large-scale profiling and prediction, and the systemic impacts of automated decisions with legal or similarly significant penalties for individuals. India's Digital Personal Data Protection Act 2023 (DPDP Act)[1] emerged as the country's first comprehensive personal data protection statute, following the landmark constitutional recognition of privacy as a fundamental right under Article 21 of the Indian Constitution [2]in Justice K.S. Puttaswamy v. Union of India[3]. The DPDP Act presented a statutory framework stablishing the rights of data principals and the obligations of data fiduciaries, comprising enhanced duties for those designated as significant data fiduciaries. However, the Act was drafted principally as a technology-neutral general data protection instrument slightly than as an explicitly AI-focused law. This generates a critical gap: the DPDP Act's provisions, while addressing foundational data protection principles, do not fully encompass the distinctive governance challenges posed by algorithmic systems, predominantly in contexts involving profiling, automated decision-making, and large-scale extrapolation operations. The central research problem animating this paper is whether a broad data protection law like the DPDP Act is normatively and institutionally suitable to address algorithmic privacy harms in its current form when associated with more specialized international regimes. The European Union's approach, exemplified by Article 22 of the General Data Protection Regulation and the newer EU AI Act with its risk-based governance framework, offers comparative benchmarks for assessing the DPDP Act's adequacy. Similarly, developing frameworks in North America, the United Kingdom, and select Asia-Pacific jurisdictions provide additional comparative perspectives on how democracies with varying

[1] DPDP, Act, 2023, s, 1.
[2] India Const. art. 21.
[3] Justice K.S. Puttaswamy (Retd.) v. union of India (2017) 10 SCC 1.

ISSN: 2582-6433

constitutional traditions and regulatory philosophies tactic the governance of algorithmic systems in relation to data protection and fundamental rights. This paper addresses three core research questions. First, to what extent do key DPDP concepts particularly data fiduciary, significant data fiduciary[4], and consent manager designations—meaningfully resemble to the algorithmic risks that foreign data protection and AI governance regimes explicitly address? Second, how do individual rights embedded within the DPDP Act[5], including access, correction, erasure, and grievance redressal mechanisms, associate functionally and substantively with the more explicit rights against solely automated decision-making found in the GDPR and the transparency and human omission safeguards mandated by the EU AI Act[6]? Third, what institutional and procedural design choices would be necessary for India to develop from a general data protection framework toward a comprehensive algorithmic privacy architecture that meaningfully addresses opacity, prejudice, and contestability while stabilizing India's constitutional commitments to dignity, autonomy, and non-discrimination? The methodology employed in this paper pools doctrinal legal analysis with comparative institutional analysis. The paper reviews the textual provisions of the DPDP Act together with the draft DPDP Rules 2025 [7]to identify how algorithmic concerns are addressed or left unaddressed by the statutory framework. This analysis is situated within India's constitutional privacy jurisprudence as developed in Puttaswamy and subsequent cases. A structured comparative analysis then evaluates the DPDP Act in contradiction of relevant international instruments, with particular attention to the GDPR's approach to automated decision-making, the EU AI Act's risk-based governance model, and select provisions from frameworks in the United Kingdom, Canada, the United States, and Singapore. Lastly, the paper incorporates a selective review of recent Indian and international scholarship addressing the intersection of artificial intelligence, data protection, and human rights to classify emerging concerns and reform proposals. The structure of this paper unfolds as follows. Part two develops the theoretical foundations of algorithmic privacy as an allowance of India's constitutional privacy framework, distinguishing among input privacy (data collection), process privacy (inference and algorithm use), and output or consequence privacy (decisions and classifications). Part three delivers an overview of the DPDP Act's key mechanisms and identifies distinctive

[4] DPDP Act, 2023, s2(4), s.10.
[5] GDPR 2016/679, art. 22.
[6] Regulation (EU) 2024/2689 of the European Parliament and of the Council of 13 June 2024 laying down rules on AI
[7] DPDP Rules, 2025, Ministry of Electronics and Information technology.

ISSN: 2582-6433

algorithmic use-cases in India's private and public sectors where these mechanisms operate. Part four grants the international benchmarks, systematically examining the GDPR, EU AI Act, and select comparator regimes. Part five undertakes the core comparative doctrinal examination, evaluating how the DPDP Act addresses scope, individual rights, data fiduciary duties, transparency obligations, state exemptions, and institutional capacity for oversight. Part six synthesizes the comparative discoveries to articulate an algorithmic privacy-oriented blueprint for India. The paper concludes by emphasizing that while the DPDP Act signifies a significant milestone, advancing Indian data governance toward algorithmic privacy protection requires targeted legislative, regulatory, and institutional reforms.

Conceptual foundations of Algorithmic Privacy

Informational Privacy and Constitutional development in India

Privacy as a fundamental right under Article 21 of the Indian Constitution persisted challenged pending the landmark judgment in K.S. Puttaswamy v. Union of India (2017) [8]decisively recognized privacy as an intrinsic aspect of human dignity and autonomy protected under the right to life and personal liberty. The Puttaswamy judgment emphasized that privacy encompasses numerous facets: bodily integrity, autonomy, informational self-determination, and psychological uprightness. For purposes of data protection and algorithmic governance, the concept of informational self-determination—the right of individuals to regulate information about themselves and to determine who accesses and utilizes such information—emerged as foundational. The constitutional acknowledgement of privacy in Puttaswamy incorporated proportionality as a essential principle governing restrictions on privacy rights. The Court held that any interruption upon privacy must satisfy a four-pronged test: first, the state action must pursue a legitimate governmental objective; second, the measure must be rationally associated to that objective; third, there must be no less obstructive substitute available; and fourth, the measure must not wholly eliminate the accurate in question. This proportionality framework, borrowed from international human rights jurisprudence, has appeared as crucial for evaluating both state and private sector data practices, particularly where algorithmic associations deployed by corporations or government interventions affect fundamental welfares. Informational privacy in the Puttaswamy framework encompasses not simply the reactive right to avoid disclosure of existing information, but the proactive right to

[8] K.S. Puttaswamy (Retd.) v. UOI, (2017) 10 SCC 1.

ISSN: 2582-6433

regulate the trajectory of one's personal data, to understand how it is being used, and to contest pronouncements derived from such data. This understanding changes beyond a passive conception of privacy-as-secrecy toward a dynamic conception of privacy-as-control and agency.

Defining Algorithmic Privacy: Three Dimensions

Building upon the Puttaswamy foundation, algorithmic privacy arises as a specialized measurement of informational privacy addressing the distinguishing challenges posed by automated data processing systems. Rather than treating algorithmic privacy as wholly detached from traditional privacy alarms, it is more analytically valuable to conceptualize it through three overlapping but distinct dimensions: input privacy, process privacy, and output or consequence privacy. Input privacy concerns the collection [9]and initial processing of personal data before algorithmic analysis. When personalities interact with digital stages, their behavioural data—clickstreams, exploration queries, location information, biometric data—are systematically bagged. Input privacy risks arise not simply when data assembly occurs without notice, but increasingly when gathering is technically legal and disclosed yet functions at a scale and granularity that individuals neither appreciate nor meaningfully switch. Algorithmic systems flourish on volumetric data acquisition; the more comprehensive the data assortment, the more influential the subsequent algorithmic models. Thus, input confidentiality in the algorithmic context necessitates not merely transparency about gathering but meaningful consent mechanisms and boundaries on collection that account for the inferential power of accumulated data. Process privacy addresses the opaque algorithmic operations through which collected data is transformed into intuitions, predictions, and classifications. Greatest algorithmic systems, mostly deep learning models used in approval systems, automated credit scoring, and predictive policing, function as "black boxes" [10]anywhere the relationship among input data and output predictions cannot be readily explicated in human-intelligible terms. This opacity generates a fundamental asymmetry: the organizations deploying these systems understand their functioning in practical terms, while affected individuals remaining ignorant of the judgement governing decisions about them. Process privacy jeopardies include not only opacity per se but also the opportunity that algorithmic models encrypt discriminatory patterns

[9] 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, 25 (2017)
[10] Frank Pasquale, The Black Box Society: The Secret Algorithms that control money and information 56(Harvard Univ. Press Cambridge, 2015)

ISSN: 2582-6433

contemporary in historical training data, amplifying societal biases in automated decisions. Additionally, algorithmic systems perform large-scale extrapolation and prediction, deriving sensitive inferences—such as health status, sexual orientation, or political affiliation—from apparently innocuous data, thereby intensifying the informational footprint of what organizations can realize about individuals far outside what individual shave directly disclosed. Output or consequence confidentiality concerns the decisions, classifications, and consequential actions taken on the basis of algorithmic predictions. Where algorithmic systems produce verdicts with legal or similarly significant belongings—such as lending decisions, hiring recommendations, insurance determinations, wellbeing eligibility assessments, or policing resource allocations—the automated decision-making itself becomes a privacy issue. [11]An adverse algorithmic pronouncement can fundamentally oblige an individual's autonomy and dignity, yet if that individual has no expressive right to understand the basis for the decision, no opportunity for human review, and no effective remedy, informational self-determination is negotiated. Consequence privacy thus encompasses not simply the data governance dimensions of input and process, but the procedural and substantive rights overriding how algorithmic outputs are translated into movements affecting individuals.

Mapping Algorithmic privacy harms to Regulatory paradigms

Numerous jurisdictions have originate up with different regulatory paradigms that have been used to counteract algorithmic privacy troubles based on their constitutional traditions, values, and regulatory philosophies. Grounded on the European data protection tradition and well-informed by the fundamental rights jurisprudence, the GDPR specifically prohibits any automated decision-making with legal or other correspondingly important consequences except exceptions apply (Article 22)[12], and requires the expressive disclosure of the logic of automated processing (Articles 13-14 and Recital 71). This methodology highlights human dignity, procedural fairness and contestability. By comparison the EU AI Act takes a risk-based methodology with AI systems being typified by the concentration of the harms they could inflict and with the obligations this imposes varyingly, where low-risk systems have negligible responsibilities and high-risk AI systems with ex-ante governance obligations[13]. With this strategy, proportionality and systemic risk management are strained. In the United States, new

[11] Sandra Watcher, Brent Mittelstadt & Chris Russell, Counterfactual Explanations without opening the Black Box: Automated Decisions and the GDPR, 31 Harv. J.L. & Tech. 841, 845 (2017)
[12] GDPR, 2016/679, art. 22, recital 71.
[13] EU AI Act, annex III.

ISSN: 2582-6433

frameworks more focused on sectoral regulation and inexpensive dynamism have given birth to disjointed solutions such as state-based confidentiality legislation and voluntary principles like the AI Bill of Rights, with a distrustful view on the ability to regulate pre-market in advance in a solitary framework. The style proposed in Canada tries to adopt a hybrid that syndicates data protection with AI-specific regulation into a single framework. India has a diverse regulatory decision: the DPDP Act, which is deliberated in greater detail below, is grounded on a wide-ranging data protection paradigm focusing on consent, transparency, and answerability of all data fiduciaries, but unambiguously does not categorize AI systems by risk and does not deliver explicit preventions of data fiduciaries on the basis of solely automated decision-making. The interpretation of such regulatory selections is based on the understanding of the influence of several conceptualizations of privacy rights, state legitimacy, and revolution incentives on algorithmic governance. The consent-and-transparency model designated by India designates a robust influence of the world-wide protection traditions, nevertheless, the regulatory bias concerning flexibility and compatibility is evident as well- India being at formerly an important AI development hub and a jurisdiction with hundreds of millions of residents at risk to algorithmic harms in credit, insurance, employment, wellbeing, and policing domains.

Overview of India's DPDP Act 2023 and Algorithmic use-cases

Key concepts and structural framework

The DPDP Act delivers the extensive data protection organization of the personal data which is based on some key perceptions. The user of personal data is known as a data principal. Personal data refers to the information that refers to a person or together with other information, a person is fairly documented. A data fiduciary is an organization that programmes the way and end use of personal data. Prominently, the Act does not make a dissimilarity amongst fiduciaries in the state and the private sector when it comes to the main necessities both of them should observe to the fundamental principles of data protection, such as rational data security, data breach revelation, and data accuracy maintenance. There are nevertheless certain segregations to certain obligations to government organizations such as storage restriction and the right to erasure due to the fear of administrative necessity and national security. Significant data fiduciary (SDF), as defined under Section 10[14] and expounded in the draft DPDP Rules

[14] DPDP Act, 2023, s, 10.

ISSN: 2582-6433

2025, refers to a data fiduciary postulated by the Central Government to process personal data on a measure where decisions made by such processor have a far-reaching consequence on the rights and welfares of the data principals. The status of an entity as an SDF leads to heightened necessities, such as requirement to have a Data Protection Officer, Data Protection Impact Assessments (DPIA)[15] annually, inspection requirements as well as, which is vital in algorithmic locations, a requirement to accomplish due diligence such that the risk of harming data principal privileges due to the deployment of algorithmic software is minimal. Specifically, the draft Rules 2025 require that SDFs provide the transparency and safety of their algorithms, keeping away those that are probable to disrupt the principles of data principality by creation discriminative pronouncements and other habits. Under the DPDP Act, there is a new body known as consent manager and this body is instructed to handle consent provided by data principals to allow nominated processing purposes. This is envisioned to solve the real-world delinquent that handling discrete consent on a large scale would be administratively compound both on the side of data principals and fiduciaries[16]. Consent manager is a mediator, who sums consent preferences and enables the withdrawal. Although such a mechanism helps to determination some transparency and control subjects, it does not change the essence of data processing, as consent is the main legitimating command, and the opportunity of withdrawal is still contemporary, but it is inconvenient in real-world circumstances. The Data Protection Board of India is the supervisor that is formed under the DPDP Act with the consultant to accept and decide complaints[17], give the remediation directions, to investigate, as well as execute the penalties of up to rupees 150 crores on SDFs, when the violation is severe. The Board includes the chairperson and the members appointed by the Central Government. Remarkably, the independence of the Board and processes of appointing members of the Board based on expertise has been a focus of plenty of academic criticism, and issues of the possible executive pressure and technical ability to govern the algorithmic systems have been expressed.

Algorithmic use-cases in Indian Private and Public Sectors

Automated credit scoring and lending decisions in fin-tech stands are also by means of algorithmic systems which are existing progressively deployed in the Indian private sector. [18]Huge alphanumeric lenders use machine knowledge models that have been accomplished on

[15] DPDP Rules, 2025, r. 12.
[16] DPDP Act, 2013, s. 2(6), s. 2(4).
[17] DPDP Act, 2023, Ch. V.
[18] RBI, Guidelines on Digital Lending, 2022.

ISSN: 2582-6433

historical borrower data to regulate creditworthiness, frequently with behavioural data on numerical platforms, mobile usage behaviours plus social network features. The human capitals and employment technology involves the use of algorithmic screening structure to filter out recommences, determine the applicant fit by examining the job explanation and even execution automated video interview investigation. Underwriting algorithms are algorithms used by insurance technology companies to determine the risk profiles and value. The advertising and endorsement systems that e-commerce platforms and arithmetical advertising setups use, based on profiling algorithm, personalize recommendations and target announcements. All of these usages include processes that involve processing of private evidence at scale, that make use of algorithmic conclusion creation that is occasionally opaque to operators, and that may be prejudiced due to preparation data biases. This is increasing in India in the framework of well-being delivery systems in the community sector, whereby government subdivisions are using algorithm applications to determine who qualifies to receive specific welfare programmes, which have led to efficiency yet also casts doubt on mistakes and exclusion. Aadhaar-based biometric identification is not necessarily an algorithmic process, in the machine learning meaning of the word, but it entails large-scale dispensation and contrast of data with unique privacy significances.[19] Facial recognition is preliminary to be used by law enforcement agencies. 3.2 Indian Private and Public Sectors Use-Cases of the Algorithms. Felonious investigation technologies and predictive police apparatuses are at an initial stage of development. Data analytics and algorithmic risk assessment are the methods used by tax authorities to detect the possible cases to be investigated. The increase in the use of algorithmic applications in the public administration makes the issue especially urgent since the actions of the government possess coercive force and impact primary interests, such as access to social welfare and individual freedom. The convergence of algorithm systems and the digital infrastructure that already exists in India will bring further complexity. The technological development model of India has focused on digital infrastructural development of the country, with its main features being Aadhaar (biometric identification), digital payment ecosystems, and growingly on the introduction of digital technologies in the service delivery process. This infrastructure, on the one hand, provides a considerable level of efficiency and inclusion, on the other hand, it allows founding a precondition of mass data gathering and algorithmic processing. The DPDP Act should operate as a regulatory tool throughout this heterogeneous ecosystem and be compatible with other digital initiatives on the infrastructure.

[19] Aadhar (targeted Delivery of Financial and Other subsidies, benefits and services) Act, 2016, No. 18 of 2016.

ISSN: 2582-6433

International benchmarks on Algorithmic Privacy

The GDPR and Automated Decision-Making rights

The General Data Protection Regulation implemented by the European Union preliminary in May 2018 is the most global pre-existing legislation on algorithmic privacy, although it was not designed as an AI-regulating tool. Article 22 of the GDPR provides an initial ban: the data subjects will have the right not to be subject to a decision made by solely automated processing, such as profiling, having legal implications with respect to them or, in other words, impacting them correspondingly in a substantial way. It is a normative ban and not a demanding ban, the rule is the appearance of an opinion to the effect that automated decision-making poses enough risks to independence and dignity that it needs to be suggested out in terms of regulation. Article 22 prohibition is used when the decisions are completed on the basis of automated dispensation only. [20]This interpretation has spawned a lot of informational disagreement. To qualify as not covered by Article 22, the human input to the decision-making process must be functional enough, as explained by the European Data Protection Board (EDPB), not purely to rubber-stamp automated recommendations but to review them and have the power to override the determination of the algorithm as well as to consider other factors that the algorithm does not take into account. This onerous criterion is an acknowledgement of the fact that nominal human intervention in the absence of authentic ability to prevail is inadequate. In Article 22, three exceptions are familiarized, namely, the automated decision-making requires for entering into or performance of a contract; the applicable law authorizes it and provides appropriate safeguards; and explicit consent is provided. Importantly, every exclusion is accompanied with added fortification in form of privileges to human intervention, opportunity to make a point of view and right to submission the decision. [21]Such architecture reflects a judgement that one should take special care when surrendering consent to automated decision-making because information asymmetries and influence differences between corporates and individuals make it impossible to grant freely and really informed consent. The practice of GDPR Article 22 has been found to be challenging to enforce, with organizations not fully complying, and not many data subjects know about this right or use it. Worldwide morals of Algorithmic privacy. However, the provision has provided a normative basis that automated decision-making is a unique privacy issue that should be specifically legally regulated. In addition to Article 22, the GDPR has transparency necessities that mean that the data subjects must be provided with

[20] GDPR, 2016/679, art. 22(1).
[21] GDPR 2016/679, art. 22(2)

ISSN: 2582-6433

meaningful information concerning automated processing logic, its relevance and its implications (Articles 13-14). [22]These provisions aim to deal with process privacy issues by introducing transparency even in the situation when automated decision-making is allowed, but does not create an unconditional "right to explanation" - a matter of significant interpretive controversy. Recital 71 states that supervisors are obliged to disclose expressive information regarding the logic of mechanical decision-making, but the Regulation is concentrating to avoid imposing the trade confidences or proprietary algorithmic information. This is an indicator of conflict between transparency (contestability and understanding needed) and intellectual property protection (needed, theoretically, to stimulate innovation). The data protection impact assessment (DPIA) approach to the GDPR also deals with the algorithmic risks. The processing is likely to lead to high risk to the rights and freedoms of individuals, which requires controllers to perform DPIAs, even in cases involving automated decision-making at scale. DPIAs involve the systematic assessment of processing reason, need, proportionality, and dangers, as well as containment tactics. Although DPIAs do not ensure the prevention of harms, they institutionalize the structured reflection of risk and require the involvement of the data protection officers and outside expertise.

The EU AI and Risk-Based governance

The EU AI Act, which assumes a new regulatory paradigm based on phases starting 2025, was a measure that adopted a fundamentally unlike regulatory paradigm to the GDPR. Instead of emphasizing data protection and individual rights, the AI Act looks to product-safety approach which looks to ex-ante guideline of AI systems based on their risk outline. The Act creates a four-level risk structure prohibited AI systems (those with unacceptable risk, like social scoring systems to categorize people as recipients of welfare benefits or jobs based on behaviour); high-risk AI systems (those that have a noteworthy impact on fundamental rights or safety); limited-risk AI systems (no particular obligations); and minimal-risk systems (no specific obligations). High-risk AI schemes are characterized, in part, by industry and in part, by application, such as AI in biometric identification and organisation, critical infrastructure administration, education and vocational training, engagement recruitment and promotion, access to vital services, law implementation, migration and asylum, justice and democratic procedures, and benefit determination. [23]The AI Act necessitates each high-risk system to have in place

[22] GDPR 2016/679, art. 13-14.
[23] EU AI Act, art. 6

ISSN: 2582-6433

comprehensive risk management systems covering the lifecycle of the AI system, data governance requirements that cover the preparation and testing datasets, documentation and record keeping, pellucidity and human supervision requirements including capability of human appraisal and intervention, and performance in real-world deployment nursing. These high-risk systems need to be registered to an EU database, they are to undergo conventionality tests as well as post-market reconnaissance by national authorities[24]. Most importantly, the EU AI Act also imposes certain requirements on benefactors of so-called general purpose AI models (GPAI models), the massive foundation models that are increasingly pouring a variety of AI applications. To safeguard that the risk in the system is identified and eliminated, the GPAI providers need to develop a risk management system, perform technical documentation, generate summaries of training data and data governance, and conduct testing. For GPAI models exhibiting even stricter obligations are imposed in the case of systemic risks through their technical capability or market coverage. The risk-based approach of AI Act is quite different to the rights-based approach of the GDPR. The GDPR states: "they are basic rights that people have and must be respected by the organizations. Artificial intelligence Act states: these types of AI systems present unique harms; this is what creators and implementers of such systems should do to avoid those harms. The two instruments are substitutes yet they act based on dissimilar logics. The AI Act does not in itself confer personal rights to challenge automated decisions but it puts in place guardrails to ensure that the most harmful automated decision-making does not take place at all.

Comparator Regimes: UK GDPR, North America, and Asia-pacific

The departure of the United Kingdom of the European Union demanded the formation of data fortification regime that was specific to the country. The UK GDPR still preserves substantive amounts of the EUGDPR, such as the Article 22 proscription against pure automatic decision-making although with some adjustments.[25] The UK Information Commissioner has on condition that extensive guidance on the rights poignant automated decision-making, and has made it clear that data questions have a right not to be the subject of an automated decision (except under certain specified conditions) as well as the right to application a human review of any automated decision (a right to human intervention which extends somewhat further than the EU version). In North America, the regulatory regime is much more decentralized and

[24] EU AI Act, annex III.
[25] Data protection Act, 2018 (UK), sch. 2, pt. 5/4

ISSN: 2582-6433

innovation-permissible. The U.S. does not have a comprehensive centralised data protection legislation, but depends on sectoral legislation (e.g., HIPAA on health data, FCRA on credit data, COPPA on children data) and new state-level legislation.[26] Rights to know, delete, and correct individual data have been introduced by the Customer Privacy Act (CPRA) of California (as well as other states) but, unlike GDPR Article 22, do not openly limit automated decision-making. Soft-law tools such as the White House AI Bill of Rights have been developed to articulate the principles of safe and operative AI systems, algorithmic accountability, data privacy, notice and clarification, and human alternatives and consideration. These principles are not legally enforceable and represent American monitoring scepticism against prescriptive ex-ante regulation. The strategy of Canada tries to strike a compromise. The PIPEDA has long absorbed on consent and reasonable safekeeping in the same direction as the DPDP Act in India. Nevertheless, the proposed Artificial Intelligence and Data Act in Canada will also provide a separate layer of AI-governance, when organizations with high-impact AI systems would have to undertake Algorithmic Impact Assessment, create a governance framework, and prove their adherence to accuracy and fairness standards[27]. The suggested Canadian model would command human checks of automatic decisions on the consequences of taking place on individuals. The approach used by Singapore in the Asia-Pacific region under the Personal Data Protection Act (PDPA) has been based on consent and accountability as it has always been the case in India. Nevertheless, the Personal Data Protection Commission of Singapore has already given some guidelines on fair and transparent AI, to deal with the problem of algorithmic bias, transparency in AI-based decisions and human intervention. Although this is not binding, it is a normative guideline to organizations based in Singapore. Australia is working on a regulatory response that puts emphasis on transparency, accountability and meaning full explanations of algorithmic decision.

Synthesis: Common Principles across regimes

Although international regimes dominating the world are organized differently and with varying philosophical orientations, they all sum up at a number of principles in the context of algorithmic privacy. First, it is widely agreed that algorithmic systems processing personal data must work in accordance with lawfulness (processing has to be lawful), purpose limitation (processing must fulfil certain purposes), proportionality (measures must be adequate to

[26] White House of science and Technology policy, Blueprint for an AI Bill of Rights (2022).
[27] AI and Data Act, Bill C-27 (Canada, 2022)

ISSN: 2582-6433

legitimate goals) and accountability (companies should prove to have complied and provide remedies to harms). Second, it is becoming acknowledged that the transparency in particular in terms of algorithmic decision-making logic, importance and implications is required, and the extent to which transparency is required (should proprietary information be disclosed or can only be high-level logic) remains a controversial issue. Fourth, it is increasingly being acknowledged that consequential automatable decisions have to be controlled by human authorities and that the mechanisms and conditions to cause human inspection are differing. Lastly, there is an agreement on the significance of combating algorithmic bias and fairness via data governance, test necessities and continuous checking.

Comparative Doctrinal Analysis: DPDP Act against International Standards

Scope and coverage of Automated Decision-Making

The main strength of the DPDP Act is that it has a gradient of data fiduciaries that is far accomplishment irrespective of the technical application. The biggest disadvantage of the Act in the algorithmic privacy background, however, is that the automated decision-making is not expressly mentioned and regulated as a separate category of processing that needs specific governance. The definition of individual data provided in the Act refers to material about an identified or identifiable person, and such definition is broad enough to refer to the algorithmic processing outputs. Nonetheless, the Act does not provide any special protection against automated decision-making with the effect of GDPR Article 22[28]. Such silence is especially important considering the economic condition in India. Within the scope of the GDPR, the restriction against purely automated decision-making was partially explained as the way of protecting individuals against organizational power imbalances in developed economies with high labour and consumer protection. India has its own set of unique problems, which are: algorithmic credit-scoring can expand rapidly in a background where formal credit history is scarce and people have no convenient way to challenge an algorithmic credit decision; expansion of enlistment algorithms in a labour surplus setting; and the use of algorithmic welfare targeting in a place where state rulings have a direct impact on access to social protection. In such cases, the lack of explicit control over automated decision-making is a void in comparison to the way of leading jurisdictions in dealing with such phenomenon. This gap is, however, to some extent covered in the draft DPDP Rules 2025. Rule 12 presents a

[28] DPDP Act, 2023 (silence on automated decisions).

ISSN: 2582-6433

requirement whereby substantial data fiduciaries take due diligence to ensure that algorithmic software that is implemented by them does not jeopardize data principal rights. This provision, although touching on algorithms transparency and safety on the regulation rule that level and not princely statute, does bring in a form of algorithmic governance that was not there before. Nonetheless, it is only imposed on SDFs and not on all data fiduciaries, and even the definition of not likely to create a risk to the rights of Data Principals is not fully specified. Is this obligation activated merely through where there has been demonstrable discrimination or is such a chance of active fairness evaluation needed? The directive on how this requirement should be fulfilled is still to be formulated in Data Protection Board practice and interpretation.

Individual rights and remedies

The DPDP Act provides some individual rights, which moderately regard the issues of algorithmic privacy, though not exhaustively. Data principals has the right of access to personal data (Section 8) which gives them the competence to access information concerning data that is maintained about them and data processing[29]. This right also has an input and process privacy purpose data principals can know what information is stored in organizations and how it is used, but the right to access does not directly provide access to the particulars of the algorithm model, the arrangement of the training data, or the performance metrics of the models. Individuals under the GDPR are entitled to more than just access to personal data under the GDPR, they must be provided with what is mentioned to as expressive information about the rationale behind automatic decision-making, this criterion goes further than access to individual data, it extends to algorithmic operations. Section 9 (right to correction) tackles the issue of accuracy and, in this way, partially takes into account that of process and output privacy. [30]When the algorithmic decision-making is strained on the basis of inaccurate information, correction rights will offer a remedy. Correction rights however deal with only data accuracy, not problematic algorithm models. Even a proficient algorithm on accurate data can give biased results in case the model is faulty, or the training material is reflective of past discrimination. This issue is directly addressed by the EU AI Act because of the focus on high-quality datasets, as opposed to a improvement right. Section 10 provides the right to erasure in the case when the retention is unnecessary, though there are exceptions to the legal compliance and performance of the contract. In the case of algorithms, the rights of erasure are not so

[29] DPDP Act, 2023, s. 8.
[30] DPDP Act, 2023, s. 9.

ISSN: 2582-6433

useful, since once data has been used to train a mechanism learning model, it is not possible to reverse engineer away the decorations that have been learned by the model. Erasure is best applicable in situations where people would like to avoid future algorithmic processing, but does not cover the damages experienced due to algorithmic decisions of the past. The right to redressal of grievances (Section 17) is the right that gives data principals the right to file complaints with Data Protection Board that allege violations. Nonetheless, the DPDP Act lacks a more defined right to human assessment of algorithmic decisions or even a right to computerised decision-making in solely automated form of Article 22 to the GDPR. The grievance redressal right is post-hoc--the algorithmic decision is previously there in place and the person must then embark on a complaint procedure. The GDPR, in its turn, defines ex-ante rights stopping as the only possible occurrence of the first instance of automated decision-making (without exceptions) and ex-post rights to human review. The grievance-redressal-oriented approach in India imposes a much greater burden on the affected people in order to regulate harms, gather evidence, make complaints and go through the dispute resolution process.

Duties of Data fiduciaries and significant data fiduciaries

The core obligations set by the DPDP Act on all data fiduciaries include sensible effort to maintain the accuracy and completeness of the data; reasonable procedures to prevent breaches of the data; notification to the affected parties as well as the Data Protection Board about the breach; and the deletion of the data in the event that no longer needs it (except in the case of government entities). Nevertheless, they do not also focus explicitly on the dangers that are unique to algorithmic processing: model bias, prediction opaqueness, and systematic discrimination. The amplified duties of material data fiduciaries form a notable innovation to doctrine which is aimed at resolving scale risks. The draft Rules require that SDFs have a Data Protection Officer in place, undertake Data Protection Impact Assessments annually, have an independent audit, and perform due diligence with respect to algorithmic systems. DPIA requirement is similar to the data protection impact valuation requirement of GDPR. Ideally, DPIAs offer a mechanism where organizations are systematic in assessing algorithmic risks and planning to mitigate[31]. Nonetheless, regulatory guidance, quality of audit, and enforcement is vital to the success of DPIAs. The GDPR practice evidence indicates that the quality of DPIA is extremely mixed: lots of organizations make DPIA as a compliance checklist instead of a

[31] DPDP Rules, 2025.

ISSN: 2582-6433

risk assessment. In the absence of robust guidance, resourcing and enforcement, the SDF audit and DPIA requirements of India may easily become formal. Both the GDPR and the EU AI Act assume very different ways of dealing with algorithmic risks using organizational responsibilities. The GDPR offers general data protection requirements on all controllers (similar to the data fiduciaries of DPDP) concerning proportionality, purpose limitation and accuracy with increased DPIA responsibilities of high-risk processing. In its turn, the EU AI Act introduces certain technical and organizational standards to high-poverty systems: risk management systems, data governance, technical documentation, conformity assessments and post-market surveillance. The approach of the AI Act is more prescriptive on what organizations should do in order to govern specifically the algorithmic systems. The SDF obligations of the DPDP Act though a momentous step in the right direction is more general and less prescriptive regarding the issue of algorithmic governance in particular. According to this comparative analysis it would help India might to go beyond general data protection to the more algorithmic privacy governance by having more specific rules explaining what algorithmic governance should look like what data governance performs SDFs need to pursue, what kind of testing and validation should be done, what they need to write down, and how they monitor algorithmic systems once they are deployed.

Algorithmic transparency and the ability to explain

Transparency is a principle that lies at the heart of data fortification and AI governance regimes yet the concept has many facets. The DPDP Act challenges transparency in terms of what data is gathered and used by the transparency responsibilities and data principal rights. But not so explicitly enclosed is transparency about the operation of algorithmic systems, what they take into account, what burdens they attach, what reasons lead to convinced outputs being generated. The protocol of transparency of computer-based decision-making delivered by the GDPR is subtle. Articles13-14 make controllers give meaningful information on the logic applied in terms of automating the dispensation, but Recital 71 specifically permits trade secrets and disclosure of intellectual property should not be made. This is a tension: valuable transparency on algorithmic reasons might need the revelation of proprietary information, but IP protection is asserted to be essential to innovation incentives. Practically, organization soften tend to give general specifications of algorithm processes without giving adequate information that allow individuals to know why various decisions were arrived at. The existing transparency requirements by DPDP Act, though integrating the requirement that data principals should have

ISSN: 2582-6433

access to personal data processing, absences clearness that transparency needs to be established in respect to algorithmic logic of decision-making. The fact that the draft Rules 2025 require SDFs to maintain algorithmic transparency in the interests of their safety is a step in the right direction yet the provision is not as clear as GDPR Article 13-14 on what transparency should be given to individuals. A right to an explanation (as opposed to a right to access information to personal data) is another notion that has spawned much academic controversy in the context of the GDPR. So, scholars maintain that a meaningful right to explanation is necessary in contestability and autonomy; others believe that explaining complex algorithmic systems can be technically impossible and that an explanation requirement can cause desirable innovation to be stifled. The EUAI Act tries to resolve this tension by separating the act of explanation based on the level of risk: high-risk systems must be transparent, documented and logged, and individuals must be notified of the use of an AI system, but the Act does not require that explanations of individual decisions should be made in real-time. The Rules 2025 in India are also deficient of providing a rapid right to explanation but redressal of complaints are also available and this may be seen as a way by which individuals may be able to seek an explanation once a decision is brought to encounter.

State exemption and constitutional proportionality

The DPDP Act provides wide exemptions on government administrations especially storage limitation (the need to delete information after the purpose has been served) and personal rights to erasure. Such exclusions are based on the issue of administrative necessity, law implementation, and national security. Rendering to the Act, these obligations shall not be applicable under the government entities or entities that process data of given purposes under government designated laws. This exemption architecture generates exclusive issues in the algorithmic setting. Government implementation of algorithmic systems in welfare delivery, law enforcement, and immigration settings creates steep privacy and dignity issues in respect to the coercive nature of state action and the regarding interests. The K.S. Puttaswamy decision held that the scope of privacy limitation did not need to meet any unreasonable requirement: it needed to pursue genuine ends, be reasonably linked with the legitimate ends, it had no alternative forms of limitation that were less disturbing, and it did not have the effect of extinguishing the right overall.[32] The wide government exemptions in the DPDP Act can be susceptible to the proportionality issues where the troubles caused to the individuals by

[32] K.S. Puttaswamy (Retd.) v. UOI, (2017) 10 SCC.

ISSN: 2582-6433

government algorithmic systems are not substantially limited. The government exemptions are a lot more specific in the EU. The GDPR extends to government processing, and the prohibition of exclusively automated decision-making in Article 22 does not have any blanket exemption of government processing provided that the processing is required to serve government purposes and appropriate protective measures are in place. The EU AI Act offers the same protection to the government use of AI, and the high-risk systems (including many government applications) have strict requirements. This comparative strategy implies that India could move in the direction of protecting the privacy of algorithms by narrowing down government exemption and placing greater oversight on the government algorithmic systems, especially where fundamental rights are at stake or a large-scale effect is involved. The constitutional proportionality model created in K.S. Puttaswamy offers a doctrinal point of connection in challenging blanket government exemptions to DPDP requirements where algorithmic systems are being implemented. In courts, it may be found that although the government agencies need exemptions to serve their legitimate purpose, the exemptions themselves should also be commensurable and cannot go to the extent of algorithmic system more than what is needed to serve the governmental purpose.

Institutional design and enforcement capacity

Under the DPDP Act, the main authority in terms of complaints adjudicators, investigators of violations, and enforcers is the Data Protection Board. Board has the powers to give compliance instructions, take undertakings of data fiduciaries, and punishments such as fines of up to rupees 150 crores in case of any substantial breach by SDFs. The institutional design of the Board casts doubts on the ability of algorithmic governance. Managing algorithmic systems demand technical skills - knowledge of machine learning model design, data science practices, measures of fairness and audit techniques. Its current staffing structure along with the composition of the Board does not at first imply a strong technical understanding of AI and data science. In comparison, the EU strategy has entailed a high employment of the data protection authorities to a wide range of technical professionals, academic researchers, and AI specialists in formulating recommendations on algorithmic governance. To enhance institutional capacity, the Board could consider the specialisation units or advisory collaboration with AI professionals, research faculty in universities and industry professionals. Moreover, independence of the Board has also been the object of academic interest. The chairperson and members of the Board are proposed by the Central Government which begs

ISSN: 2582-6433

the question of potential executive influence especially relating to government entities where the algorithmic systems of entities are complaint to. The GDPR methodology offers more independence to data protection authorities in their form of collegial governance and multi-stakeholder authorities at the member state level. India can reinforce algorithmic governance by improving independence of the Board and allowing the multi-stakeholder input in algorithmic governance standards.

Towards Algorithmic privacy blueprint for India

Identified systemic gaps

Part Five shows that the architecture of the DPDP Act suffers four systemic gaps when considered through the prism of algorithmic privacy. To begin with, the Act offers an unimpressive direct acknowledgement of automated decision-making as a unique challenge to governance. Contrasting the GDPR, in Article 22, with the high-risk classifications in the EU AI Act, the DPDP Act has no primary-statute that deals with automated decisions resulting in legal or other similarly meaningful outcomes. [33]The draft Rules deal with this by partially means of SDF requirements about algorithmic transparency, but the main statute is technology-neutral and does not provide ex-ante safeguards against abusive automated decision-making. Second, the Act contains no independent right to explanation or post-hoc human review of algorithmic decisions. The grievance redressal rights of data principals are post-hoc redress first assert able once decisions have been made. The GDPR puts in place ex-ante rights of not only automated decision-making and ex-post rights of human review. The strategy of India puts a great deal more responsibility on the aggrieved to find solutions. Third, the Act offers some restricted direction on the assessment of algorithmic impacts and audit. Although the draft Rules also require the DPIAs and audits of SDFs, the rules do not state the nature of the algorithmic governance practices, what testing and validation should involve, or how algorithmic fairness and non-discrimination should be assessed by auditors. Fourth, these blanket government exemptions in the DPDP Act could not sufficiently limit the use of algorithmic systems in situations related to the public sector, which can impact fundamental rights, because such exemptions are subject to litigation, which poses an unpredictable restriction on affected vulnerable populations in the interim.

[33] Supra note 12.

ISSN: 2582-6433

Reform agenda: Literature, Regulatory, and Institutional Layers

To fill these gaps a multi-layered reform agenda is needed that would comprise legislative changes, regulatory rule-making and institutional capacity-building. At the legislative level, a focused amendment to the initial DPDP law can bring out a directive clause solely concerning automated decision-making only in high-impact situations. This provision does not have to do the same that GDPR Article 22 does and explicitly require explicit consent before algorithmic systems are deployed to make decisions that affect employment, credit, insurance, welfare, or public policing, [34]but may instead outline that significant data fiduciaries ought to have explicit consent before making such decisions unless otherwise permitted by law. The amendment could create a right to human review and challenge of consequential algorithmic decisions, which would entail that people should now be notified of algorithmic decision-making, of their right to seek human review, and should be provided with adequate information to challenge the decision in a meaningful way. On the regulatory rule-making tier, Data Protection Board must create more specific guidance on the standards of algorithmic governance of SDFs, what practices should be regarded as the appropriate approach to governing data in an algorithmic system, what pre-deployment testing and validation need to be done, what metrics of fairness should be tracked, and what records should be kept at organizations. Such guidance may be developed in terms of sectoral codes of practice, such as different guidance on the AI use in financial services, employment, insurance, and public welfare. It should include codes of input privacy (what is the appropriate level of data collection to train algorithms and use them), process privacy (what are testing and monitoring to find and mitigate algorithmic bias required), and output/consequence privacy (what is the protection of consequential decisions). The Board is supposed to create standards and measures of audit of the algorithms, which are performed by the independent auditors, such as audit protocols, audit qualification, and audit reporting. On the institutional level, the Data Protection Board ought to set up an AI and algorithmic governance unit, with technical specialists and data scientists, as well as experts in AI ethics. The Board ought to create and sustain systems of algorithmic risk evaluations, as is the high-risk classification framework enforced in the EU AI Act, which recognizes groups of algorithmic uses that merit increased scrutiny by the scale of the potential harms, and the underlying interests involved. The Board ought to create a sandbox system where organizations would experiment with new algorithmic applications that are governed by the regulations, can be monitored and limited, permitting responsible innovation without harming people. The

[34] GDPR, 2016/679, art. 22.

ISSN: 2582-6433

governance structure of the Board should be improved to be more independent and multi-stakeholder, which may be by creating an advisory board that may include the representatives of the civil society, academia, industry, and the affected communities.

Sectoral Implementation: Finance, Employment, Insurance and Public administration

Privacy authority should be algorithmic but paid sector-specific consideration to understand exceptional risks and contexts in numerous domains. The algorithmic credit-scoring and lending decisions in the financial services have far reaching implications on the economic engagement of individuals. The sectoral code is required to establish that financial institutions perform algorithmic impact assessments prior to implementing new credit-scoring models, evaluate disparate impact-assessment models across covered characteristics, and undertake continuous monitoring of model-performance by demographic group and provide individuals with mechanisms to comprehend the causes of adverse credit decisions and request human review. [35]Financial algorithmic systems at risk may need to be pre-approved by the Data Protection Board or regulator of the sector. Systems of algorithmic recruitment and performance evaluation determine the access of livelihood of individuals in employment. The sectoral code must mandate that recruitment algorithms must be periodically assessed to determine their discriminatory effect, automated screening models must be verified to forecast job performance in reality, that job seekers should be aware of algorithmic use, and that algorithmic job performance appraisals should be challengeable by employees. Since India has high surplus of labour, algorithmic discrimination in the job market poses severe dangers of exclusion at the systemic level. Algorithms of risk assessment and pricing of insurance influence economic security in the insurance sector. Sectoral code must require disclosure of aspects that affect risk-assessment, prohibit the use of proxies in place of character that are shielded, a requirement that the algorithmic models be actuarially verified and the individuals being able to access human scrutiny of the determination of insurances. Algorithms used in the delivery of welfare, law enforcement, and immigration raise unique issues in the context of public administration, due to the coercive power of the government and the underlying fundamental interests involved. The use of algorithmic systems by government agencies must be accompanied by increased transparency requirements, a requirement of human review of the consequences of particular decisions, and periodic audit. Courts must be on the lookout in

[35] RBI, Master Direction- Non- banking financial company- Systematically important Non-Deposit taking company and deposit taking company (RBI) Directions, 2016.

ISSN: 2582-6433

terms of whether government algorithm systems meet constitutional proportionality requirements. According to the government the wide-ranging exemptions in some DPDP duties should not protect the algorithmic systems against relevant monitoring.

Conclusion

The Digital Personal Data Protection Act 2023 is an historic legislative step forward by making India the first country to have a constitutional regime of personal data protection and constitutional acknowledgment of privacy as a fundamental element of dignities and interests in independence. Consent, transparency, and accountability in the DPDP Act give the framework of operations that can be used in various data processing situations. Nonetheless, the Act can be found to be wanting when interpreted in the context of algorithmic privacy the unique issues of automated decision-making, profiling, and massive inference functions. Although the Act applies to all data fiduciaries despite technological implementation, it does not expressly recognize automated decision-making as a governance priority, does not impose ex-ante protections against purely automated decisions, only remedies through grievance redressal, and does not give much institutional direction on algorithmic transparency, fairness evaluation, and audit. These holes are even more acute as compared to the DPDP Act and the international regimes that have come out clearly to discuss algorithmic governance. The Article 22 of the GDPR banning the use of automated decisions alone and requiring transparency on the logic behind the algorithmic decisions creates personal rights against algorithmic obscurity and decision-making freedom. The risk-based governance approach of the EU AI Act, which places AI systems in categories based on the harm they could cause and sets more gradual requirements, offers organizations an excellent insight into the nature of AI governance: general data protection cannot be the sole responsibility of such systems, and they should have a separate framework of rules. The decision of the Indian policy to follow a general data protection tool instead of an AI-specific law is not surprising, as it is informed by the apprehensions of regulatory quality and the compatibility with innovation as well as institutional capability. Nevertheless, such option must not exclude specific amendments or regulatory elaboration of algorithmic privacy principles into the framework of DPDP. This paper comparatively examines several areas of convergence of international regimes in terms of core principles: lawfulness, purpose restriction, proportionality, and accountability in algorithmic processing; transparency in relation to algorithmic decision-making and its implications; human capacity to oversee consequences in relation to algorithmic decisions;

ISSN: 2582-6433

systematic risk control and reduction; and increased protections of algorithmic systems on fundamental rights. India has an opportunity to develop its algorithmic privacy framework by selectively implementing the following principles through ex-ante protection of high-impact algorithmic systems, a general regulatory guidance, specifying algorithmic governance practices, institutional capacity-building in the Data Protection Board, codes of sectoral implementation of domain-specific risks, and proportionality-impaired government exemptions. In addition to instrumental issues of governance, algorithmic privacy protection has strong constitutional adherence to human dignity, autonomous self-determination, and protection against discrimination. The decision in Puttaswamy described privacy in terms of intrinsic part of the human dignity and autonomy the right to define the path of personal data and to appeal decisions that impact oneself. Opaque systems of algorithmic operation, which make it possible to discriminate, which centralize decisional power in organizations or government agencies and which provide individuals with no significant recourse, undermine these constitutional promises. On the other hand, the requirements of transparency, fairness, human oversight, and individual contestations can potentially serve positive functions, such as allowing access to credit by individuals with limited credit histories, enabling effective welfare provision to the needy, and promoting good-grounded governance, and avoiding individual autonomy and dignity India is on a crossroad. It is also a huge hub of AI development and innovation, and at the same time a jurisdiction with hundreds of millions of citizens exposed to algorithmic harms in credit, insurance, employment, welfare, and policing, and a constitutional democracy dedicated to fundamental rights and dignity. The policy decisions taken in the next 2-3 years on the interpretation and application of the DPDP Act, as well as the guidance provided by the Data Protection Board and whether targeted legislative reforms are undertaken, will have significant impacts on whether algorithm development in India will proceed with meaningful protection of human dignity and autonomy or whether vulnerable groups will continue to experience an unequal number of risks of algorithmic discrimination and exclusion. The paper supports an algorithmic privacy-focused solution, which would combine the global experience gained in GDPR and EU AI Act and consider the constitutional system of India and the practical developmental issues. This would be a message to the planet that India takes the issue of AI innovation seriously in regard to basic rights- a template especially relevant in a global society where the majority of the citizens of AI-influenced jurisdictions do not have robust policies and frameworks safeguarding their rights to algorithms. This conclusion ends up representing a belief that dignified, independent

ISSN: 2582-6433

personhood is both not a luxury item that needs to be uploaded by rich democracies only, but a right that must and should be defended at all jurisdictions and societal settings.