ALGORITHMIC BIAS AND DISCRIMINATION UNDER INDIA'S DPDPA: EVALUATING THE ADEQUACY OF LEGAL FRAMEWORKS FOR AI-DRIVEN DECISION-MAKING

Neha Verma, LLM, Gujarat National Law University, Silvassa Campus

ABSTRACT

Artificial Intelligence (AI) systems are progressively inducted across India's various sectors like financial sector, hiring processes, healthcare delivery, policing, welfare distribution, and public governance. While AI-driven decision-making promises efficiency and neutrality, several domestic and global developments demonstrate that such systems may embed and amplify discrimination. India's Digital Personal Data Protection Act, 2023 (DPDPA), although a major step toward personal data governance, contains no explicit provisions regulating algorithmic bias, automated profiling, or the fairness of AI systems. The present article evaluates whether the DPDPA provides adequate safeguards against algorithmic discrimination and examines its limitations in comparison with the European Union's GDPR and the EU AI Act. Drawing upon recent international case law and emerging Indian experiences, the present article argues that India's existing legal regime including DPDPA is insufficient to regulate discriminatory AI practices. Additionally, the article clarifies that while the Act functions as the data protection legislation, in India it was not specifically designed to govern AI underscoring its importance in tackling AI-related challenges. The article concludes by recommending policy amendments, including evaluations of algorithmic effects mandates for human supervision and a unified structure for AI responsibility consistent, with the constitutional rights outlined in Articles 14, 15 and 21.

INTRODUCTION

AI plays a role in India's shift towards digitalization. AI technologies are swiftly shaping the availability of opportunities and essential services including algorithm-based recruitment, predictive policing, automated credit evaluations and medical diagnostics. Yet global research and Indian pilot initiatives reveal that AI systems are not impartial; instead they often intensify systemic inequalities embedded either during their creation or, within historical data. This issue is demonstrated by a number of incidents documented in the US, UK, and EU: discriminatory employment algorithms, biased tenant-screening instruments, and defective biometric identification systems have previously led to legal action and regulatory action.

India's implementation of AI in administration be it via Aadhaar verification algorithm-based welfare allocation or the trial deployment of generative AI, in the judiciary raises the issue of algorithmic bias as a matter of constitutional significance. However, the DPDPA, India's data protection legislation centers on notice, consent, storage and breach responsibilities. It does not regulate profiling or automated decision-making. Consequently, a regulatory void exists that permits AI systems to impact rights without undergoing any legal scrutiny.

This article examines whether the DPDPA is adequate to address algorithmic discrimination in India and situates the analysis within a comparative global context. It contends that in order to shield people from algorithmic injustice, India has to implement a rights-based, open, and auditable AI regulatory framework.

COMPREHENDING ALGORITHM BIAS

A. BIAS

Bias typically refers to depending on stereotypes or presumptions about groups defined by race, gender, ethnicity or related characteristics. In the United States these differences linked to identity are termed "suspect classes", in constitutional law. They receive protection under the Equal Protection Clause, which is enforced via the Fifth Amendment for matters and the Fourteenth Amendment for matters involving states. When a law treats one group differently from others, courts apply a certain level of judicial review: strict scrutiny, intermediate scrutiny, or rational basis review, depending on which group is involved.

Statutes that create classifications for instance undergo rigorous scrutiny. This requires the government to prove there is a justification, for the unequal treatment and that the approach taken is precisely aimed at achieving that justification. Conversely distinctions based on gender face scrutiny, where the government needs to establish that the classification furthers an important government objective by means that are substantially related to achieving that objective. A statute might lead to a claim of impact even when it appears neutral at first glance if it disproportionately disadvantages a protected category. For example, a recruitment algorithm that repeatedly prefers one group, over another could expose the employer to a disparate impact legal challenge. The

Within AI the word "bias" is comprehended in a sense to encompass both deliberate and accidental inclinations—whether aware or unaware—that can skew the correctness of an AI model or its outcomes. Bias encompasses a range of tendencies that impede impartial judgment and technical accuracy. Crucially AI bias also denotes flaws, in system architecture or training datasets that degrade the quality of the results. Because AI models are designed by humans who choose the datasets for training the developers' personal beliefs and biases may be unintentionally incorporated into the algorithm from the beginning. This inadvertent bias is frequently difficult to identify since it is integrated into the system's framework or the foundational data. Consequently, those making decisions might overly rely on AI-produced results that are influenced by biased data.

Regarding the issue of bias judges ought to be aware of four main factors, from the beginning.

With respect to the risk of algorithmic bias, there are four principal considerations that judges should recognize at the outset.[1]

a. Judges (and the law) use the term bias in a different and more specific way than computer engineers. For AI specialists, algorithmic bias refers broadly to the difference between an algorithm's output and the desired outcome, not necessarily to bias of the

[1] An Introduction to Artificial Intelligence for Federal Judges by James E. Baker Laurie N. Hobart Matthew Mittelsteadt at page 33.

sort addressed by the equal protection clause.

b. Algorithmic bias can be caused by human prejudice of the sort courts typically address, cognitive bias of the sort behavioral scientists typically address, design and data flaws of the sort computer engineers address, or all of the above.

c. As bias is defined above, there is no such thing as a bias-free algorithm. There is a tendency to believe that "numbers are neutral" and present objective truths, but numbers may produce erroneous results.[2]

d. Through careful engineering, thoughtful use of data, and adjusted algorithmic weights, it is possible to create AI systems with lower margins of error. [3]It is also possible that reducing one form of bias by adjusting, for example, the underlying analytical framework or data sets can allow other forms of bias to creep in.

As the guardians of evidentiary standards, judges have the authority to limit or exclude unreliable or biased AI evidence by posing the appropriate preliminary inquiries. Developing the ability to ask such questions requires a clear understanding of the various ways in which algorithmic bias may manifest.

B. ALGORITHM BIAS

Algorithms are fundamentally a precise and comprehensive set of instructions, crafted to generate solutions to the problems they were created to address. They offer an automated approach to performing calculations and computational operations. Basic algorithms operate using a linear approach to problem solving, whereas more intricate algorithms incorporate conditional functions that enable them to perform more complex tasks, now referred to as automated decision-making (ADM), aimed at achieving automation for tasks that previously necessitated oversight or additional human resources. Currently, numerous Artificial Intelligence Software (AIs) have included Automated Decision-Making systems (ADMs) to enhance their operational capabilities

[2] Joni R. Jackson, Algorithmic Bias, 15 J. of Leadership, Accountability & Ethics 55–65 (2018), https://search.proquest.com/docview/2170233068?accountid=14214

[3] Jake Silberg & James Manyika, Notes from the AI Frontier: Tackling bias in Artificial Intelligence (and in Humans), McKinsey Glob. Inst. (June 6, 2019), https://www.mckinsey.com/featured-insights/artificial-intelligence/tackling-bias-in-artificial-intelligence-and-inhumans

in judicial systems worldwide.[4]

C. FORMS OF ALGORITHMIC BIAS

The United Nations Institute for Disarmament Research suggests several categories and sources of algorithmic bias.[5]

1. Statistical bias - Statistical bias takes place when an algorithm's predicted results differ from a statistical benchmark, like the true occurrence rate of real-world events.[6]

2. Moral bias occurs when an algorithm's output differs from accepted norms (regulatory, legal, ethical, social, etc.)[7]. Consider a hiring algorithm that is used to evaluate job candidates. Candidates from more flexible or unconventional backgrounds may be unfairly disadvantaged, even if they are equally qualified, if it is designed to give preference to applicants who have worked for organizations with rigid, traditional workplace cultures. Because the algorithm implicitly favors some workplace principles (such as rigid hierarchy or formality) over others, possibly limiting varied opinions, this indicates a moral bias.

3. Training data bias. Like humans, AI learns from experience; however, its experience is based exclusively on data, often hand-selected by a human developer. Inaccuracies or misrepresentations in this data can perpetuate biases by embedding them in algorithmic code.[8]

4. Inappropriate focus occurs when an algorithm's training data are ill-suited to the algorithm's task.[9]

5. Inappropriate deployment happens when a system is used in a context for which it was

[4] Neha Bharti & Mohd Imran Algorithm bias and Discrimination bias in AI-Assisted Legal Processes International Journal of Law Management & Humanities [ISSN 2581-5369] Volume 8 | Issue 2 2025
[5] United Nations Institute for Disarmament Research (UNIDIR), Algorithmic Bias and the Weaponization of Increasingly Autonomous Technologies: A Primer, 9 UNIDIR Resources (2018), http://www.unidir.ch/files/publications/pdfs/algorithmic-bias-and-theweaponization-of-increasingly-autonomous-technologies-en-720.pdf.
[6] Id. at 2.
[7] Id.
[8] Id. at 2–3.
[9] Id. at 4.

not designed, tested, and validated.[10]

6. Interpretation bias occurs where an algorithm's output is confusing or subject to incorrect interpretation by those working with the technology.[11]

7. Unwitting human bias occurs when human preferences, stereotypes, values, fears, or knowledge are unintentionally embedded into an application. For instance, an engineer might use technical ideas to develop the risk model in an algorithm intended to forecast risk. But since risk is a subjective concept, the algorithm is likely to represent the particular anxieties, risk tolerances, and viewpoints of those who created it.

8. Intentional bias is when scientists, operators, or decision-makers purposefully utilize AI tools like facial recognition or prediction algorithms to target vulnerable or marginalized populations. Social traits like ethnicity, gender, sexual orientation, nationality, religion, handicap, and more can be identified and classified using these algorithms. In China, for instance, people with physical characteristics linked to the Uighur ethnic group have been identified and tracked using facial recognition technology. The question of whether it is ever appropriate to purposefully employ social identification identifiers as search criteria is raised by this targeting, which is detrimental. The answer may depend on factors like the intended purpose, how "search parameter" is defined, and the degree of human oversight involved.

D. SOURCES OF BIAS

There are three major sources of algorithmic bias:[12]

a. Data Bias: Occurs when training datasets reflect historical prejudices, stereotypes, or underrepresentation of certain communities. For instance, if past hiring data shows a preference for male candidates, an AI model trained on such data may learn to replicate and reinforce gender bias. [13]

b. Design Bias: Emerges from the unconscious assumptions or values embedded in

[10] Id.
[11] UNIDIR, supra note 33, at 5
[12] Dr. Subholaxmi Mukherjee, Algorithmic Bias and Discrimination: Legal Accountability of AI Systems Jul - Aug 2025 IJIRMPS | ISSN: 2349-7300 Volume 13 Issue 4.
[13] Id

the structure or logic of an algorithm. This may happen when developers fail to account for social diversity or overlook intersectional vulnerabilities during system design and testing.[14]

c. Feedback Loops: Arise when biased outcomes from algorithms are fed back into the system as new data, reinforcing and amplifying the original distortions. This is especially common in predictive policing or credit scoring, where past biased decisions influence future risk assessments.[15]

This phenomenon occurs because algorithms influence other algorithms with their recommendations and forecasts shaping real-world conditions. An example is when an algorithm's crime predictions alter police officer behavior, subsequently affecting crime detection. Newly detected crimes were then incorporated into the system. Such feedback loops are prevalent, and many machine learning systems inherently include them.[16] The algorithmic bias has both technical and constitutional implications relevant to Articles 14 and 15.

ILLUSTRATIVE CASE STUDIES OF ALGORITHMIC BIAS

The concrete threats AI systems bring to justice, equality, and constitutional rights are illustrated by real-world instances of algorithmic bias. These cases demonstrate how AI can purposefully or inadvertently reinforce prejudice, highlighting the critical need for extensive legal protections beyond those provided under India's DPDP Act.

a. COMPAS Recidivism Algorithm (United States)[17]

The U.S. Criminal justice system widely employs the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) algorithm to predict the likelihood of reoffending. A 2016 ProPublica investigation revealed that when controlling for similar criminal histories COMPAS more often categorized Black defendants as high risk for recidivism than white defendants. This racial bias raised

[14] Id.
[15] Id.
[16] Report on Bias in Algorithm Artificial Intelligence and Discrimination, European Union Agency for Fundamental Rights,2022 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2022-bias-in-algorithms_en.pdf
[17] Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). *ProPublica*. Retrieved from https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

concerns about responsibility, equity and transparency, in automated judicial decisions emphasizing the potential dangers of uncritically relying on opaque AI tools.

b. Amazon's AI Recruiting Tool (United States)[18]

To streamline recruitment Amazon developed an AI- hiring tool. Nonetheless the algorithm exhibited gender bias by favoring candidates over female ones. This happened because the system was trained on hiring data that was mainly male, which unintentionally perpetuated and intensified gender disparities, in recruitment. After uncovering the bias Amazon discontinued the tool emphasizing the risks of training data and the importance of actively mitigating bias.

c. UK'S AGORITHMIC WELFARE DECISIONS[19]

Individuals with disabilities and ethnic minority groups were disproportionately affected by the UK governments use of techniques to detect benefit fraud within the Universal Credit system. Because of the systems flawed profiling vulnerable populations were wrongfully. Penalized, leading to public backlash and legal disputes. This case underscores the risks posed by AI technologies, in social welfare initiatives, which can perpetuate societal inequalities if not properly monitored or safeguarded for fairness.

d. FACIAL RECOGNITION AND UIGHUR SURVEILLANCE (CHINA)[20]

Chinese officials employed facial recognition technology to surveil individuals of the Uighur group enabling human rights abuses. The intentional deployment of AI, for profiling highlights significant ethical and legal issues globally showing how algorithmic systems can serve as instruments to oppress marginalized communities.

e. AADHAAR AND ALGORITHMIC WELFARE TARGETING (INDIA)[21]

[18] Dastin, J. (2018). *Reuters*. Retrieved from https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G
[19] Butler, P. (2020). *The Guardian*. Retrieved from https://www.theguardian.com/society/2020/dec/10/universal-credit-errors-welfare-fraud-algorithm-targeted-disabled-people
[20] Mozur, P., & Zhong, R. (2019). *The New York Times*. Retrieved from https://www.nytimes.com/2019/01/21/technology/china-surveillance-uighurs.html
[21] Drèze, J., & Khera, R. (2017). *Economic & Political Weekly*, 52(41). Retrieved from https://www.epw.in/journal/2017/41/special-articles/exclusion-errors-aadhaar-based-welfare-targeting.html

> In India trial applications of Aadhaar data integrated with AI technologies for welfare allocation have resulted in exclusion mistakes, where vulnerable groups were wrongfully barred from receiving services. These cases expose the difficulties of implementing AI in environments without legal safeguards for equality and anti-discrimination underscoring deficiencies, in the DPDP Act's ability to protect constitutional rights.

These instances together demonstrate the varied aspects of algorithmic bias highlighting the necessity of creating clear legal structures that focus on AI transparency, responsibility and equity.

CURRENT LEGAL FRAMEWORKS AND LIMITATIONS

In the landmark 2017 *Puttaswamy v. Union of India*[22] judgment, privacy was established as a fundamental right under Article 21 of the Indian Constitution including personal control over data and obtaining informed consent for its utilization. However AI technologies frequently bypass these safeguards via methods like inference-based profiling, use of data and automated decision processes posing a challenge, to the efficacy of consent-based data protection frameworks. To address these issues the Digital Personal Data Protection (DPDP) Act 2023 was introduced to create a framework for the protection of digital personal data. It should be noted that although the DPDP Act regulates data protection it does not serve as AI governance legislation; nonetheless it continues to be the legal framework indirectly influencing AI-associated data protections, in India.

The DPDP Act regulates the gathering and handling of personal information covering activities within the country as well as some extraterritorial operations. It requires notification and consent that is informed and can be withdrawn while providing individuals with rights to access rectify, delete and seek remedies for their data. Data Fiduciaries are obligated to guarantee purpose and storage constraints uphold data accuracy apply security protocols and promptly report any breaches. Additionally, the Act establishes Significant Data Fiduciaries, who face rigorous requirements, like conducting Data Protection Impact Assessments and appointing a Data Protection Officer. Authority is granted to the Data Protection Board of India which has

[22] Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. (2017) 10 SCC 1.

the power to probe infringements and levy financial fines.

While the DPDP Act represents advancement it fails to sufficiently tackle the security issues uniquely presented by AI technologies. In contrast to regulations that identify algorithmic inference as a distinct privacy concern the DPDP Act handles all data processing uniformly neglecting the particular risks associated with AI. It misses AI-related threats, like non-transparent decision processes, self-directed data inference and the ability of AI systems to derive or reconstruct sensitive information. These AI functions enable the use of information in manners that bypass conventional notice-and-consent mechanisms undermining the autonomy safeguarded by Article 21. The limitations of the Act also relate to Article 14 which guarantees equality under the law and protects against conduct by the state or private entities. Without provisions, for fairness and non-discrimination the DPDP Act is poorly suited to address bias.

Similarly, Article 15—which forbids discrimination based on factors like religion, race, caste, gender and birthplace—is contested by AI-based profiling systems that can deduce these characteristics. The DPDP Act does not oversee damaging automated profiling methods in contrast, to the EU, UK, China and OECD regulations, which clearly restrict discriminatory AI behaviours.

In general, the Act offers constitutional safeguards because it does not address algorithmic inference, data repurposing, model bias, automated decision-making or AI transparency. This deficiency grows more critical as India rapidly advances its use of AI, in administration welfare distribution and law enforcement.

GLOBAL APPROACHES

Although India's DPDP Act 2023 sets up a structure for safeguarding personal data its approach to AI concerns contrasts with international frameworks that explicitly address algorithmic profiling harms from automation and biased results. In comparison to norms India's framework is more focused on privacy than AI providing robust fundamental protections but limited measures, for algorithmic responsibility.

A. EUROPEAN UNION

The General Data Protection Regulation (GDPR) of the European Union continues to be the

worldwide privacy standard. Its advantages comprise:

a. Stringent regulations on automated decision processes granting people the right to avoid decisions made exclusively through automated methods when those decisions have an impact, on them.

b. Mandatory Data Protection Impact Assessments (DPIAs) for high-risk processing, including AI systems.

c. Clear safeguards, against profiling that could lead to results.

The Artificial Intelligence Act of the European Union extends its scope by:

a. Creating risk-based categories (unacceptable, high, limited, minimal)

b. Imposing transparency, fairness, and human oversight requirements.

c. Banning AI Systems that involve biometric categorization by sensitive traits

d. mass surveillance, and discriminatory profiling.

The DPDP Act has no similar rights to contest automated decisions, no AI risk classifications, no prohibitions on high-risk AI uses, and no explicit protections against discriminatory profiling. Thus, India's framework lags significantly behind the EU in linking privacy, equality, and AI ethics.

B. UNITED STATES 'S SECTORAL APPROACH & EMERGING AI REGULATORY STANDARDS

The United States does not have a federal privacy statute but implements sector-specific rules, like HIPAA (health) COPPA (children's data) and FCRA (credit scoring). Nevertheless, regarding AI governance:

a. The White House AI Bill of Rights (2022) establishes guidelines for efficient AI safeguards, against algorithmic bias and provides for notification and the option to opt out of automated systems.

b. The NIST AI Risk Management Framework (2023) offers recommendations, on

reducing bias ensuring transparency and maintaining accountability.

c. Multiple state regulations (such, as Californias CCPA/CPRA) grant rights concerning automated decision-making.

While less consolidated the U.S. Dedicates resources to AI risk reduction and anti-discrimination measures. In contrast Indias DPDP Act lacks safeguards, against algorithmic bias or AI-related discrimination rendering Articles 14 and 15 exposed.

C. UNITED KINGDOM'S DATA PROTECTION ACT 2018 & AI SAFETY INITIATIVES

Following Brexit, the UK preserved GDPR standards via the DPA 2018 encompassing:

a. Explicit rules on automated decision-making,

b. Mandatory explanations for algorithmic outcomes,

c. Data Protection Impact Assessment for AI use,

d. Furthermore, the UK spearheads worldwide AI safety efforts, including the Bletchley Declaration (2023) and the creation of an AI Safety Institute dedicated to addressing threats, like AI autonomy, inference and systemic bias.

India does not have a framework for AI oversight and its DPDP Act fails to cover algorithmic transparency or human-, in-the-loop protections areas that the UK emphasizes.

D. CHINA'S PERSONAL INFORMATION PROTECTION LAW (PIPL) & AI-SPECIFIC REGULATIONS

The PIPL, in China comprises:

a. Strong rules on data minimization and purpose limitation,

b. Requirements for transparency in automated decision-making,

c. The right to demand explanations and reject automated profiling.

China has additionally implemented rules concerning algorithmic recommendation systems (2021) and generative AI (2023) emphasizing:

a. Bias prevention,

b. Data quality,

c. Algorithmic transparency,

d. State oversight of high-impact AI applications.

China's regulatory structure is more focused on AI. Imposes stricter rules on managing biased and non-transparent systems. In contrast India's DPDP Act lacks requirements resulting in deficiencies, in safeguarding equality (Art. 14) And preventing discrimination (Art. 15) Against AI-related threats.

E. OECD AND GLOBAL SOFT LAW FRAMEWORKS

The **OECD AI Principles (2019)**[23] endorsed by more than 40 nations emphasize:

a. fairness,

b. transparency,

c. safety,

d. accountability,

e. human-centric AI.

These guidelines shape international regulatory frameworks and emphasize the significance of safeguarding individuals, against discrimination and privacy breaches caused by AI.

India conceptually aligns with OECD privacy principles. Its DPDP Act neither incorporates obligations related to fairness or explainability nor governs high-risk AI implementations.

[23] OECD AI Principles overview https://oecd.ai/en/ai-principles

Therefore, India's DPDP Act, 2023. Safeguards informational privacy, yet it fails to explicitly tackle privacy threats emerging from AI-based inference or automated data handling thus restricting the complete fulfilment of Article 21 protections. Furthermore, the Act does not incorporate measures to prevent bias resulting in shortcomings, in upholding the equality and non-discrimination promised under Articles 14 and 15. In contrast, to the approaches used in the EU, UK, China and developing U.S. Guidelines the Act lacks clear provisions regarding automated decision-making, algorithmic openness or equity. Additionally, it does not create an AI regulatory body require AI-specific impact evaluations nor ban high-risk or damaging AI activities leading to a framework that is mainly centred on general data protection instead of full AI oversight.

CONCLUSION AND RECOMMENDATIONS

The swift growth of AI technologies has introduced regulatory issues at the crossroads of privacy, fairness and non-discrimination. India's DPDP Act 2023 provides a structure for safeguarding personal data and is grounded in the constitutional acknowledgment of privacy under Article 21. However, comparisons, with strategies reveal that robust AI regulation usually demands further protections targeting algorithmic inference, automated decisions, transparency and discrimination hazards.

Although India has built a foundational privacy structure it presently does not have AI-specific protections that numerous global frameworks deem crucial for avoiding algorithmic damage. To bring India's environment in line, with global best practices and constitutional rights a number of focused policy measures are required.

Policy Recommendations

a. Mandatory Algorithmic Impact Assessments (AIAs):

   Implement AIAs for every high-risk AI application—particularly in areas such as welfare provision, law enforcement, recruitment and financial services. These evaluations must assess threats to privacy, fairness, bias and procedural fairness aligning with standards like those in the EU AI Act and Canada's Directive, on Automated Decision-Making.

b. Dedicated AI Regulatory Authority:

c. Create a national AI regulatory authority—akin to the EU AI Office or the UK AI Safety Institute—to supervise AI governance, certification, surveillance and adherence. This organization should establish criteria, for fairness, openness, precision and responsibility.

d. Rights Against Automated Decision-Making:

   Include rights allowing people to: request evaluation of automated choices; receive clarifications, for algorithmic results; contest biased or incorrect AI decisions. These safeguards are crucial to maintain Articles 14, 15 and 21.

e. Regulation of AI Profiling and Sensitive Inference:

f. Strictly control AI technologies that deduce sensitive characteristics (caste, religion, gender, health, ethnicity), without obtaining consent. This type of profiling threatens equality and non-discrimination. Should be managed via legal protections.

g. Transparency and Explainability Standards:

h. Mandate that AI systems— those used by governmental entities—reveal their fundamental algorithms, details about training data, confidence levels and error statistics. Transparency is essential, for upholding responsibility.

i. Mandatory Data Protection & AI Safety Audits:

   AI models with impact must be subject to regular evaluations to identify biased behaviors, errors, in accuracy and potential security risks. Such assessments ought to be performed by external organizations.

j. Prohibition of Harmful or Unjustified AI Uses:

   Introduce statutory bans on practices such as social scoring, mass surveillance AI, or emotion recognition in policing—mirroring global prohibitions found in the EU AI Act and OECD guidelines.

k. Integration of OECD, UNESCO & G20 AI Principles into Domestic Law: India ought to integrate international AI ethics standards into its laws to set defined

guidelines, for fairness, responsibility, human supervision and risk reduction.

l. Strengthening DPDP Act Provisions for AI:

The DPDP Act could be updated via amendments or related rules to clearly govern:

I. algorithmic bias,

II. discriminatory outputs,

III. automated profiling,

IV. AI-generated sensitive inferences,

V. opaque decision-making processes. This would enhance constitutional compliance and bring India closer to global AI governance norms.

As India continues expanding its digital and AI ecosystem, adopting these policy reforms would help construct a rights-based, transparent, and accountable AI governance structure. Embedding AI-specific protections within the DPDP framework or through a dedicated AI law will ensure constitutional alignment with Articles 14, 15, and 21 while keeping pace with global regulatory evolution.