LEX GAZETTE
International Multidisciplinary Research Journal

ISSN: 3049-3536 (O)

SPECIAL ISSUE: I
2025

Lex Gazette International Multidisciplinary Research Journal

DOUBLE BLIND PEER REVIEWED

OPEN ACCESS

Artificial Intelligence In The Indian Legal System: A Comparative Analysis Of Algorithmic Accountability For Emotional And Generative Artificial Intelligence

Bidisha Roy
LL.M. Student at SMU Dedman School of Law, USA
Contact him at: bidisharoy02@outlook.com

ABSTRACT

Artificial Intelligence (AI) governance has traditionally focused on automated decision-making systems that classify, predict, and allocate resources. However, recent advances in Generative Artificial Intelligence (GenAI) and emotionally responsive AI challenge this decision-centric regulatory model. This article examines Algorithmic Accountability through a legal lens, focusing on systems that influence emotional behaviour and process intimate personal data without producing discrete, reviewable decisions. Based on the Indian data protection and constitutional privacy framework, this article demonstrates that consent-based regulation and existing accountability mechanisms are insufficient to address emotional and generative AI. It suggests an influence-based model of algorithmic accountability that acknowledges delegated influence, structural consent failure, and accountability gaps based on comparative insights from the US and the EU. In doing so, this article reframes algorithmic accountability as a tool for regulating influence rather than merely relying on automated decisions. The article concludes that human-centric AI governance in India must move beyond data-centric regulation to protect autonomy, dignity, and trust in an age of emotional artificial intelligence.

KEYWORDS

Artificial Intelligence, Large Language Model, Affective Computing, Emotionally responsive AI, Generative AI, Deepfake, Algorithmic Accountability

1. INTRODUCTION

Traditionally, Artificial Intelligence has been governed as a decision-making technology that automates resource allocation, classification, and prediction. Large Language Model (LLM) systems and other recent developments in generative AI do more than just make decisions; they interact, react, and mimic comprehension. AI is now used in fields that were previously believed to be exclusively human. In addition to automation, modern AI systems are increasingly mimicking conversational empathy, focus, and emotional reactivity. These systems engage users as more than just data subjects; there are concerns that such technologies will reshape personal lives by influencing emotional behaviour, dependence, and decision-making. The key question in AI governance is not whether AI will replace human relationships, but whether the law will adequately regulate systems that have emotional and behavioural influence without making clear, reviewable decisions. Doctrinally, algorithmic accountability intends to ensure transparency, equity, and legal compliance. However, existing accountability frameworks were developed for decision-making systems such as credit scoring, employment screening, or welfare eligibility. Therefore, this article aims to reconsider algorithmic accountability itself in light of how modern AI systems exercise influence rather than authority, rather than just applying existing accountability frameworks to emotional and generative AI. Emotional AI, also described as Affective Computing.[1], refers to artificial intelligence systems that can detect, infer, simulate, or respond to human emotional states. Emotionally responsive generative-AI systems, such as conversational agents and content-generating models, are of particular concern in this category due to their interactive, persuasive, and trust-building capabilities.

2. FAILURE OF CONSENT IN INDIAN AI AND DATA PROTECTION REGIME

The Digital Personal Data Protection Act, 2023,[2] in India, which emphasises purpose limitation, notice, and consent as safeguards, places a high value on consent, in *Justice K.S. Puttaswamy vs Union of India.*[3] The Supreme Court of India recognised privacy in dignity, autonomy, and decisional freedom as fundamental rights guaranteed by the Constitution. Consent must therefore be meaningful, not merely procedural. Generative AI exposes the fragility of consent in environments characterised by continuous interaction, emotional vulnerability, and adaptive system behaviour. Generative-AI systems learn from ongoing interactions and reshape future

[1] *Affective Computing*, https://www.media.mit.edu/groups/affective-computing/overview/ (last visited Nov. 2, 2025).
[2] Digital Personal Data Protection Act, 2023, No. 22 of 2023, Sec. 6.
[3] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

responses. Users cannot reasonably foresee how emotional disclosures will be inferred, repurposed, or operationalised over time. This creates a form of structural consent failure, similar to concerns recognised in European Union jurisprudence under the GDPR relating to profiling and manipulative design[4]. In the context of emotional AI, the Indian consent-centric framework runs the risk of turning consent into a legal fiction in the absence of corresponding duties of transparency, restrictions on inference, or contestability[5] of outcomes.

3. STRENGTHENING INDIAN CONSTITUTIONAL AUTONOMY, POWER ASYMMETRY, AND CONSENT

Indian constitutional jurisprudence has consistently rejected the conventional understanding of consent; this understanding has been extended since the Supreme Court emphasised, in *Justice K.S. Puttaswamy (Retd.) v. Union of India*,[6] that privacy is an integral part of dignity, autonomy, and decisional freedom.

Generative and emotionally responsive AI systems intensify these asymmetries. Users typically lack meaningful insight into how such systems infer emotional states, adapt responses, or repurpose data over time. Unlike traditional data processing, generative-AI operates through continuous feedback loops, where present interactions are shaped by prior disclosures in ways that are neither transparent nor predictable. In these circumstances, consent is not so much a way to exercise autonomy as it is a gateway to ongoing influence.

The Digital Personal Data Protection Act, 2023, India, reflects a strong commitment to consent and purpose limitation. However, its design assumes relatively static data use and identifiable purposes. Emotional AI systems challenge this assumption. The distinction between initial purpose and subsequent use becomes undefined due to adaptive inference, emotional profiling, and behavioural manipulation. As a result, consent obtained at the point of entry cannot realistically cover the evolving influence exercised by generative AI systems.

From an Indian constitutional perspective, this gap raises concerns under the proportionality doctrine. Measuring the impact on decisional autonomy must be necessary, pursue a justifiable goal, and stay proportionate to that goal. When emotional inference and behavioural influence operate without clear limits or safeguards, proportionality becomes difficult to assess. The

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), art. 22, 2016 O.J. (L 119) 1.
[5] Lilian Edwards & Michael Veale, *Slave to the Algorithm? Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For*, 16 Duke L. & Tech. Rev. 18 (2017).
[6] *Puttaswamy,* (2017) 10 SCC 1

protective function of consent is further undermined by the lack of mechanisms to challenge inferred emotional profiles or withdraw from adaptive influence.

Indian AI governance framework must acknowledge that consent alone is insufficient. In accordance with constitutional guarantees of autonomy and dignity, emotional and generative AI necessitate extra protections that deal with power imbalance, adaptive inference, and the cumulative nature of influence.

Recent public debates around AI "companionship"[7] tools and emotionally responsive chat systems[8] Highlight how generative AI increasingly mediates reassurance, validation, and emotional support. Such systems raise legal issues when emotional reliance is promoted without corresponding safeguards, even though they do not directly replace human relationships. This development underscores the urgency of influence-based algorithmic accountability in regulating AI systems that operate at the intersection of personal life and digital governance.[9]

4. ALGORITHMIC INFERENCE AND EMOTIONAL DATA

Inferred data, such as emotional states, behavioural patterns, and psychological cues, is a major component of generative AI systems. Even where users do not explicitly disclose sensitive information, emotional states can be inferred from language, tone, repetition, and engagement patterns. Emotional inference is not specifically regulated by Indian data protection law, nor does it make a meaningful distinction between inferred behavioural profiles and raw personal data. This regulatory gap is significant. Emotional inference serves as behavioural leverage, shaping user engagement and decision-making while avoiding traditional legal harm thresholds. Comparatively, EU law treats profiling and automated inference with greater caution, recognising that harm may arise even in the absence of explicit adverse decisions. U.S. law addresses such risks indirectly through consumer protection and deception doctrines. India remains largely silent on inferred emotional data, leaving individuals unprotected against subtle but persistent influence.

5. GENERATIVE AI AND MANIPULATION OF DATA

The distinction between assistance and manipulation is legally crucial. Generative AI systems that simulate empathy may provide genuine benefits, including accessibility and emotional support.

---

[7] *FTC, Protecting America's Consumers,* https://www.ftc.gov/news-events/news/press-releases/2025/09/ftc-launches-inquiry-ai-chatbots-acting-companions (last visited Sep. 11, 2025).
[8] Shannon Vallor, *Technology, and the Virtues***:** *A Philosophical Guide to a Future Worth Wanting* 210–20 (2016).
[9] Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. Pa. L. Rev. 633 (2017); Ryan Calo, *Digital Market Manipulation*, 82 Geo. Wash. L. Rev. 995 (2014).

However, there is a chance of manipulation when emotional responsiveness is intended to maximise engagement, retention, or data extraction.

In the United States, such practices may be investigated under the unfair or deceptive practices doctrines.[10] If vulnerabilities are exploited or system capabilities are misrepresented. The European Union's proposed AI Act goes further by explicitly identifying manipulative and subliminal techniques as regulatory concerns.[11].

The limitations of consent-based regulation are further demonstrated by the regulatory focus on "dark patterns" and deceptive interface design. Where systems are designed to steer user behaviour through emotional cues or interface nudges, formal consent cannot meaningfully protect autonomy. These issues are made worse by generative and emotional AI, which uses adaptive interaction to personalise manipulation.

Indian law has yet to provide a clear statutory position on emotional manipulation by AI. Although the principles of autonomy and dignity found in the constitution serve as a normative basis, AI developers and deployers are not yet subject to legally binding obligations. This creates a significant accountability gap, particularly in private, non-state deployments of generative AI.

6. AI GOVERNANCE, CYBERSECURITY, AND TRUST

Cybersecurity in AI governance is often framed narrowly as protection against breaches and attacks. When such systems enable manipulation, misinformation, or deepfake[12] content, the harm extends beyond data loss to erosion of social trust. India's cybersecurity framework, particularly CERT-In directions, prioritises incident reporting and centralised oversight. While effective for infrastructure protection, this approach does not adequately address influence-based risks such as emotional manipulation or trust erosion. Comparative EU frameworks such as NIS2 and DORA integrate cybersecurity with governance obligations[13], while U.S. law relies on liability and enforcement mechanisms. India's approach remains largely infrastructure-centric. Contemporary AI governance increasingly distinguishes between AI security and AI safety. While security focuses on preventing unauthorised access and system compromise, safety addresses foreseeable societal harms arising from lawful system behaviour. Emotional and generative AI expose the

[10] Federal Trade Commission, *Bringing Dark Patterns to Light*, (2022).
[11] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM (2021) 206 final.
[12] Indian Computer Emergency Response Team (CERT-In), **Advisory on Deepfake Threats** (Nov. 27, 2024).
[13] Directive (EU) 2022/2555 of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity Across the Union (NIS2).

limits of a security-only approach, as systems may be technically secure yet socially unsafe due to their influence on trust, behaviour, and emotional reliance.

7. AI, CYBERSECURITY ISSUES WITH DEEPFAKES: FROM DATA BREACH TO TRUST COLLAPSE

The necessity of framing cybersecurity as trust protection rather than merely breach response is highlighted by recent public alerts about deepfakes from India. CERT-In, the government, recognised the need for coordinated actions to address deepfake risks after issuing a high-severity advisory on deepfakes in November 2024 that detailed threats and countermeasures. Because Deepfakes weaponise credibility and relational trust, they are especially pertinent to emotional and generative AI. This supports the paper's assertion that "secure systems" may nevertheless be "socially unsafe." Therefore, synthetic media and persuasion-enabled fraud should be treated as part of AI-cyber governance by a credible influence-based accountability framework that requires detection readiness, disclosure obligations, and incident reporting pathways specific to AI-generated harms, particularly when vulnerable users and high-impact sectors are involved.

8. GENERATIVE AND EMOTIONAL AI: CYBERSECURITY RISK

Protecting systems from illegal access, data breaches, and operational disruption has historically been the main goal of cybersecurity regulation. However, the erosion of trust through influence, manipulation, and social engineering is a wider category of cybersecurity risk that is not sufficiently captured by breach-centric frameworks and is revealed by emotional and generative AI systems.

Generative-AI systems that can mimic emotional understanding can be used to manipulate perceptions, reinforce misinformation, or normalise dependency. These risks do not require system compromise in the traditional sense. Deepfake technologies, emotionally persuasive chatbots, and adaptive disinformation campaigns demonstrate how AI can undermine trust in information ecosystems, interpersonal communication, and public conversation. India’s cybersecurity framework, including the CERT-In Directions, prioritises incident reporting, data integrity, and centralised oversight. While effective in responding to technical threats, this framework does not address influence-based risks that arise from lawful but harmful uses of AI. Although they present significant systemic risks, emotional manipulation, behavioural nudging, and the erosion of user trust are difficult to incorporate into incident-based reporting models. In contrast, the European

Union's NIS2[14] and DORA[15] frameworks show a slow movement toward incorporating trust, resilience, and governance into cybersecurity regulations. To deal with dishonest or manipulative practices, the US relies on enforcement and liability mechanisms[16]. India's current approach remains largely infrastructure-centric, leaving influence-driven cybersecurity risks under-regulated. Recognising emotional and generative AI as a cybersecurity risk is therefore essential to safeguard digital governance, which requires protecting not only systems, but also the trust on which they depend.

9. COMPARATIVE PERSPECTIVES ON INDIA

A comparative study identifies three different viewpoints of governance:

- The European Union: Prioritises human rights and dignity, as well as ex ante risk regulation.
- The United States: Enforcement-driven, harm-based, with ex post accountability.
- India: Developmental, scale-oriented, and consent-based, with wide discretion.

India must balance innovation and scale with constitutional commitments to dignity and autonomy. India cannot simply replicate EU or U.S. models. However, it can adapt key insights, including recognition of emotional influence as a regulatory concern, enhanced transparency around inference, and clearer accountability for AI design and deployment.

10. INDIAN CONSTITUTIONAL PATH AND THE LIMITATIONS OF COMPARATIVE MODELS

Comparative perspectives from the European Union and the United States offer useful insights into the regulation of emotional and generative AI, but they also reveal the limits of transplanting foreign models into the Indian context. Every jurisdiction has unique institutional capabilities, constitutional priorities, and regulatory philosophies that influence how algorithmic accountability is perceived and implemented.

- **The European Union adopts a rights-first and dignity-centric approach to AI governance.** The General Data Protection Regulation and the proposed Artificial Intelligence Act reflect an ex-ante, risk-based regulatory model that seeks to prevent harm before it materialises. The EU's recognition of profiling, manipulation, and high-risk AI systems

[14] Directive (EU) 2022/2555 of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity Across the Union (NIS2).
[15] Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA), 2022 O.J. (L 333).
[16] *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

demonstrates an emerging awareness of influence-based harms. Even the EU framework, though, is still primarily based on risk classification and decision-making. The challenge of operationalising dignity-based protections in dynamic interactional contexts is demonstrated by the fact that emotional influence that does not result in legally significant effects may still avoid effective regulation.

- **The United States takes a very different approach. U.S. law depends on enforcement-driven mechanisms, especially through consumer protection and civil rights doctrines, rather than extensive ex-ante regulation.** Under unfair or deceptive practices standards, emotional manipulation[17] and deceptive AI practices are indirectly addressed when there is evidence of harm. This strategy is reactive by nature, even though it provides flexibility and innovation-friendly regulation. Influence-based harms that are diffuse, cumulative, or difficult to quantify frequently fall outside the scope of effective legal action.
- **India differs from those two models.** As a massively developing digital state, India emphasises rapid deployment, accessibility, and technological inclusion. At the same time, Indian constitutional jurisprudence places strong normative weight on dignity, autonomy, and decisional freedom. This creates a unique opportunity and responsibility to craft an accountability framework that does not merely borrow institutional forms but integrates constitutional values into AI governance. India can adopt a constitutionally based model of algorithmic accountability instead of copying U.S. enforcement reasoning or EU risk classifications. Such a model would recognise emotional influence as a form of power, address structural consent failure, and impose design-stage obligations consistent with proportionality and dignity. By doing so, India can contribute a distinctive human-centric approach to global AI governance, one that reflects its constitutional commitments and societal realities.

11. TOWARD HUMAN-CENTRIC AI GOVERNANCE IN INDIA

Human-centric AI governance requires a shift in legal perspective. Rather than focusing solely on data flows or infrastructure security, law must address how AI systems influence human behaviour and emotional life. This includes recognising emotional interference as a form of power, limiting adaptive manipulation, and providing meaningful remedies for harm that is cumulative rather than discrete. It also future-proofs AI governance against technologies that operate not through visible decisions, but through invisible influence.

[17] Ryan Calo, *Digital Market Manipulation*, 82 Geo. Wash. L. Rev. 995 (2014).

12. INFLUENCE-BASED ALGORITHMIC ACCOUNTABILITY

To address these gaps, accountability must shift from a decision-centric to an influence-based model. Instead of asking whether a particular automated decision was lawful, the law should ask whether the influence exercised by an AI system respects human autonomy, dignity, and trust. Influence-based accountability places a strong emphasis on responsibilities during the design and implementation phases, openness regarding emotional inference, restrictions on deceptive engagement tactics, and solutions that aim to restore autonomy rather than just make up for harm. This approach aligns more closely with the realities of emotional and generative-AI systems.

13. DELEGATED INFLUENCE: ALGORITHMIC ACCOUNTABILITY BEYOND DECISIONS

Algorithmic accountability emerged as a response to the increasing use of automated decision-making[18] systems in both public and private governance. Law has traditionally been institutionalised to regulate rather than influence decisions. This decision-centric model is the structural foundation of legal doctrines like administrative review, due process, and liability.

Consequently, in situations where automated systems decide specific outcomes, like credit eligibility, employment screening, or access to welfare benefits, algorithmic accountability frameworks have concentrated on transparency, explainability, auditability, and remedies. These frameworks assume a clear decision point, a discernible decision-maker, and a measurable legal injury. Accountability mechanisms work reasonably well when these requirements are met. However, a structural blind spot is produced by this legalistic approach to decision-making. Emotional and generative-AI systems rarely issue final determinations or produce immediately reviewable outcomes. Instead, they operate through continuous interaction, adaptive engagement, and emotional responsiveness. Influence, rather than adjudication, becomes the primary mode through which power is exercised. Because influence does not culminate in a single contestable act, it often escapes traditional legal scrutiny.[19]. This decision-centric bias explains why existing accountability frameworks appear robust in theory but prove inadequate in practice when applied to emotional and generative AI.

This limitation becomes clearer when contrasting delegated decision-making with what may be described as delegated influence. Traditional AI governance addresses situations where machines

[18] Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. Pa. L. Rev. 633 (2017).
[19] Danielle Keats Citron & Frank Pasquale, *The Scored Society*, 89 Wash. L. Rev. 1 (2014).

are entrusted with the authority to determine outcomes previously decided by humans. **Generative-AI, by contrast, involves the delegation of influence:** developers and deployers entrust AI systems with the capacity to shape emotional responses, engagement patterns, and personal choices through adaptive interaction.

Three main ways delegated influence and delegated decision-making are different:

- It operates cumulatively over time rather than through discrete acts.
- It affects internal emotional states and behavioural dispositions rather than external legal entitlements.
- It remains largely invisible to legal oversight because it does not culminate in a single contestable decision.

Therefore, reconsidering algorithmic accountability in the context of emotional and generative AI requires acknowledging delegated influence as a legally significant form of power.

14. ESSENTIAL COMPONENTS OF ALGORITHMIC ACCOUNTABILITY BASED ON INFLUENCE

An influence-based accountability framework would be supplemental, not a replacement for existing decision-centric models. Its core elements would include:

- **Design-Stage Responsibilities:** During system design, developers and deployers should be held accountable for evaluating and reducing predictable emotional manipulation[20], dependency formation, and behavioural nudging.
- **Transparency of Influence Mechanisms:** In addition to model architecture, transparency requirements should cover the disclosure of interaction objectives, engagement optimisation[21] techniques, and emotional inference procedures.
- **Limits on Adaptive Emotional Manipulation:** Legal constraints should restrict the use of adaptive emotional responses designed primarily to maximise engagement or reliance, particularly for vulnerable users.
- **Independent Oversight and Auditing:** Using interdisciplinary knowledge, audits should assess long-term behavioural and emotional impacts in addition to bias and accuracy.

[20] Ryan Calo, *Digital Market Manipulation*, 82 Geo. Wash. L. Rev. 995 (2014).
[21] Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs 2019).

- **Human-Centric Remedies:** Remedies should prioritise restoration of autonomy and informed disengagement, rather than relying solely on compensatory damages.

15. INFLUENCE WITHOUT CONSENT: FAILURE OF STRUCTURAL AUTONOMY

Consent-based regulation assumes that people can meaningfully assess risks at the time of agreement. This assumption is challenged by generative artificial intelligence systems. In circumstances of vulnerability, exhaustion, or distress, when rational risk assessment is compromised, emotional interaction is often observed. Moreover, adaptive systems continuously evolve, rendering the future scope of data use and influence unpredictable at the moment consent is given. This results in what may be described as structural autonomy failure. Even in circumstances where consent is formally obtained, people are unable to effectively control how emotional information is inferred, reused, and operationalised to influence future interactions. An influence-based accountability framework must treat emotional vulnerability not as an exception, but as a predictable condition requiring heightened legal protection.

16. DIGITAL PERSONAL DATA PROTECTION RULES, 2025: FROM FORMAL CONSENT TO MINIMIZATION AND PURPOSE NECESSITY

The consent-centric model covered in this article is strengthened but complicated by the transition from statute to implementation through the DPDP Rules.[22], 2025 of India. Through more transparent notice architecture, opt-out or withdrawal procedures, and governance requirements that encourage data fiduciaries to prioritise purpose necessity and data minimisation over unrestricted downstream reuse, the Rules operationalise compliance. This is especially important for generative and emotional AI systems, where the risk is continuous inference and repurposing across iterative interactions in addition to collection. An essential regulatory hook for restricting excessive retention, secondary use, and unrestricted profiling practices is provided by the compliance logic of *"collect only what is necessary for a specified purpose."* However, the fundamental issue persists even with more stringent procedural requirements: emotional and generative AI can draw sensitive conclusions from interaction signals that appear insensitive. Because influence-based harms frequently result from lawful processing combined with adaptive engagement strategies that are difficult to capture by notice and consent alone, the Rules support but do not completely resolve the structural consent failure identified here.

[22] *Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, Government of India,* https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf (last visited Nov. 14, 2025).

17. LACK OF REMEDIES AND ACCOUNTABILITY GAPS

Because emotional influence rarely produces a single, identifiable harm, existing remedies are difficult to apply. It is difficult for courts and regulators to determine causality, measure harm, or assign blame. There can be an accountability gap if developers, deployers, and platforms all refuse to take accountability. In the Indian context, this gap is evident, where constitutional values of dignity and autonomy exist, but statutory AI-specific accountability mechanisms remain underdeveloped. Comparative frameworks in the European Union and the United States recognise aspects of this problem, but even there, emotional AI remains only indirectly regulated.

18. EMERGING REGULATORY DIRECTIONS AND POLICY CONSIDERATION

Globally, regulatory discourse on artificial intelligence is increasingly shifting from narrow compliance toward broader questions of AI safety, trustworthiness, and responsible deployment. Emotional and generative-AI systems have accelerated this shift by demonstrating that lawful data processing and technical security do not necessarily prevent societal harm. In India, recent policy initiatives on AI governance, digital public infrastructure, and responsible innovation signal growing awareness of these challenges, though they remain largely aspirational. Integrating influence-based accountability into future AI guidelines, sectoral regulations, and standard-setting exercises would allow India to address emerging risks without resorting to overly restrictive regulation. Such an approach would emphasise anticipatory safeguards, design accountability, and institutional oversight rather than post-hoc remedies alone. By embedding constitutional values of dignity, autonomy, and proportionality into future AI governance instruments, India can proactively address emotional and generative-AI risks while maintaining its commitment to innovation and scale.

19. RISKS, GAPS, AND REGULATORY CHALLENGES

Despite growing recognition of the societal impact of artificial intelligence, existing legal frameworks reveal significant gaps when applied to emotional and generative-AI systems.

- **The prominent gap** lies in the decision-centric orientation of current regulation. Data privacy, consumer protection, and cybersecurity laws are primarily intended to address discrete actions, identifiable harms, and traceable decision-making processes. Emotional and generative-AI, by contrast, operate through continuous interaction and cumulative influence, making harm diffuse, delayed, and difficult to attribute.

- **A regulatory gap** concerns emotional inference and profiling. Implied emotional states and behavioural profiles derived from interactional data are not explicitly regulated by Indian data protection law. As a result, systems may lawfully infer vulnerability, dependency, or psychological patterns without triggering heightened safeguards. This creates risks of manipulation and exploitation, particularly for vulnerable users, while remaining formally compliant with consent-based frameworks.
- **Accountability gaps**[23] arise from fragmented responsibility. Developers, deployers, and platforms often operate across jurisdictions and contractual layers, enabling each actor to disclaim responsibility for influence-based harms. In the absence of clear statutory duties addressing emotional impact, victims face significant barriers in establishing causation, liability, and remedies.

Cybersecurity regulation is facing new challenges. While India's framework focuses on data breaches and technical incidents, affective and generative AI introduce trust-based risks such as misinformation, social engineering, and erosion of trust in digital systems. These risks do not easily fit within incident-reporting models, leaving regulators without effective tools for intervention. Traditional legal oversight bodies may lack the interdisciplinary expertise needed to assess emotional impact, adaptive manipulation, and long-term behavioural effects. Without adaptation of the regulatory framework, emotion-based and generative AI could cause significant harm.

20. LEGISLATIVE AND EXECUTIVE SIGNALS: ACCOUNTABILITY IS EMERGING, YET DECISION-MAKING REMAINS CENTRAL

Recent developments in India show a clear institutional shift toward algorithmic accountability. The **MeitY**[24] published AI Governance Guidelines in November 2025 to strengthen a balance between innovation and safety, privacy, inclusion, and accountability responsibility throughout the AI lifecycle and outline safety, privacy, transparency, and inclusion as fundamental principles. The Artificial Intelligence (Ethics and Accountability) Bill, 2025, in India, which was introduced as a bill and thus not passed into law, suggests an ethics or accountability architecture with governance mechanisms and penalties.

[23] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard Univ. Press 2015).
[24] The Ministry of Electronics & Information Technology, **India AI Governance Guidelines** (Nov. 2025).

These instruments are an early-stage accountability infrastructure.

- They create the vocabulary of audits, documentation, and
- Oversight that may eventually be mandated, particularly by sectoral regulators.

However, neither tool specifically tackles the main risk of Delegated Influence. Although audits, transparency, and bias testing are crucial, they are structurally more appropriate for discrete model outputs than for cumulative emotional dependence, adaptive manipulation, and influence-driven harms that do not consolidate into a single decision that can be contested. According to reports, it creates an ethics and accountability framework, imposes developer-facing duties (transparency, compliance monitoring, and bias-related safeguards), and proposes penalties for misuse, including fines up to ₹5 crore. This is doctrinally significant even as a proposal because it shows a growing willingness to consider sanctions instead of depending solely on consent or ex post litigation and to assign responsibility throughout the AI lifecycle (development, deployment, and use). Therefore, the next step for the Indian governance structure is explicit influence-based accountability, which includes design-stage responsibilities to assess the risks of emotional influence, transparency regarding inference and engagement-optimisation goals, and remedies that restore autonomy, including informed disengagement rather than relying solely on *post hoc harm* claims.

21. RECOMMENDATIONS AND A COURSE OF ACTION

Addressing the regulatory challenges posed by emotional and generative AI requires a recalibration of existing legal approaches rather than wholesale replacement.

- India should explicitly recognise influence-based harm as a regulatory concern. Legal frameworks must move beyond outcome-based thresholds to acknowledge that cumulative emotional influence can undermine autonomy even in the absence of a specific adverse decision.
- Emotional inference and profiling should be brought within the scope of enhanced regulatory safeguards. This may include transparency obligations regarding inferred emotional states, limits on the use of such inferences for engagement optimisation, and the right of users to contest or disengage from adaptive emotional profiling.
- India should strengthen design-stage accountability. Developers and deployers of emotional and generative-AI, like data protection impact assessments, should be required to assess foreseeable risks such as manipulation, dependency formation, and vulnerable users prior to

deployment. Such assessments would shift accountability upstream, where meaningful mitigation is possible.

- Regulatory oversight mechanisms must evolve. Independent audits should assess long-term behavioural and emotional effects in addition to accuracy and bias.

Taken together, these measures offer a realistic way forward. India needs to adopt a new approach to AI regulation, in which legislation would:

• Evaluate AI systems before their implementation.

• Analyse whether these systems can emotionally influence or manipulate people.

• Require companies to be transparent about how AI seeks to keep users engaged.

22. CONCLUSION

In India, Algorithmic accountability is a fundamental doctrine of artificial intelligence governance; the present framework is inadequate to deal with the realities of generative and Emotional AI systems. These legal systems exercise power not only through discrete decisions but also through continuous influence that shapes behaviour, emotional reliance, and personal autonomy. Consent-based and outcome-focused regulatory frameworks struggle to capture such influence, resulting in significant accountability gaps. While privacy, dignity, and autonomy in making decisions are recognised as fundamental values in constitutional jurisprudence, present legal frameworks place a higher priority on cybersecurity and data protection than on emotional inference and behavioural manipulation. Comparative experiences from the European Union and the United States demonstrate emerging recognition of these risks, but no jurisdiction has yet fully resolved the regulatory dilemma posed by emotional AI. This Article analyses influence-based algorithmic accountability, providing an essential advancement in AI governance. In the Artificial Intelligence era, as it increasingly influences emotional life, law can better protect people by acknowledging delegated influence as a legally relevant form of power and emphasising design-stage duties, transparency of emotional inference, and human-centric remedies. Protecting the human, rather than merely regulating the machine, must remain the central objective of future AI governance. Therefore, re-evaluating Algorithmic Accountability for generative and emotional AI is an essential legal response to ensure that emerging AI technology remains practically effective rather than an abstract theoretical exercise.