LEX GAZETTE
International Multidisciplinary Research Journal

ISSN: 3049-3536 (O)

VOLUME: II, ISSUE: I
JANUARY (2026)

Lex Gazette International Multidisciplinary Research Journal

DOUBLE BLIND PEER REVIEWED

OPEN ACCESS

Artificial Intelligence As An Inference Infrastructure: Recasting The Right To Privacy Across Surveillance, Profiling And Generative Systems In India

Gayatri Rathi
Research Scholar at the Faculty of Law, Swami Vivekanand Subharti University, Meerut
Contact at: gayatrirathi950@gmail.com

Dr. Sarika Tyagi
Associate Professor at the Faculty of Law, Swami Vivekanand Subharti University, Meerut
Contact at: tyagisarika21@gmail.com

ABSTRACT

The use of Artificial Intelligence in India is growing, as is its potential to generate assessments related to identity, risk, credibility, eligibility, and reputation from data that is often under-utilized. This poses a significant challenge to privacy in India as current privacy laws in India address primarily data collection and processing. Consequential harm is primarily caused by automated systems that generate assessments and synthesize data. This paper considers whether the privacy provisions in the Indian Constitution, surveillance laws, the responsibilities of intermediaries and the Digital Personal data Protection Act, 2023 address these issues. This study employs a doctrinal approach. It examines existing provisions in the Constitution, the Public Interest Litigation and Landmark judgments, existing Statutes, Executive Orders, and select literature related to profiling, model inversion, membership inference, and generative systems. The study found that the protection of proportionality under Article 21 of the Constitution of India addresses these issues and the other provisions of the Act would provide limited rights to contest the inferred data. Indian privacy laws provide insufficient protection against automated decision-making, and fragmented measures against deepfakes and model leakage. The paper further suggests that privacy-inferenced data should be subjected to constraint of purpose, audit, and review

KEYWORDS

Artificial Intelligence, Digital Personal Data Protection Act, Deepfakes, Indian Telegraph Act, Right To Privacy, Inference Infrastructure

1. INTRODUCTION

Artificial intelligence in Indian governance and markets should not be viewed in terms of isolated applications, but as an inference infrastructure that transforms the disjointed into the meaningful. The primary privacy harm is often perceived to occur after the legal collection of data. It is when systems derive identities, intents, risks, credibility, reputation, and eligibility from behavioral remnants, communication metadata, biometrics, and digital traces. Surveillance systems produce suspicion scores and social association networks, while profiling systems attribute predicted characteristics and generative systems synthesize representations that can function as evidence or be attributed as speech. These outputs can produce more direct social and legal impacts than the original data. A privacy framework of concealment, consent, and control of disclosed information results in an enormous regulatory vacuum, as invasive finalizations can be drawn from public, anonymized, or legally collected data [1], [2]. The Digital Personal Data Protection Act, 2023 mandates the governance of digital personal data, yet its sufficiency is contingent on whether the constraints of purpose, fiduciary responsibilities, and the right of individuals are extended to downstream inferences that impact dignity and autonomy as encapsulated in Article 21.

This article proposes the idea of ‘inference infrastructure’ as a legal framework to combine surveillance, profiling, and generative systems. It seeks to ascertain if the Indian constitutional right to privacy, as well as the existing statutory duties, can inhibit the production, distribution, and operational use of high-impact inferences, beyond the first stage of data collection. This study adopts a doctrinal approach and interprets Article 21, leading privacy judgments, interception powers, the obligations of intermediaries, and the Digital Personal Data Protection Bill, 2023, in relation to the technical structure of contemporary inference pipelines. Rule 3(1)(b) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, reflects a concern of governance in relation to privacy breaches, impersonation, and deceptive attribution [3] [4]. The thesis of this study is that these Rules, and the provisions of the DPDP Act, should be interpreted in the context of contestability and purpose and outcome proportionality when an inferred characteristic or an artificially generated representation significantly alters a person's status, rights, standing, or reputation.

2. CONSTITUTIONAL ARCHITECTURE OF PRIVACY IN INDIA

Responses to physical surveillance, the aggregation of published information, and state data systems are how the Indian judiciary has developed the right to privacy. Within the context of these rulings, the pertinent doctrinal question is not if the judiciary anticipated the implications of modern artificial intelligence, but if the principles of these rulings can evaluate the implications of constant observation, categorization, prediction, and dictation of behavior. Article 21 provides protection to dignity, autonomy, and personal liberty. Articles 14 and 19 provide protections against arbitrary classifications and against restrictions on the rights of free speech and free association, respectively. The harm of cumulative inference is obscured by a focus on specific intrusions, since a person could be classified numerous times, with no single classification appearing to be the most important [5], [6]. The focus of the constitutional cases analyzed in this section is on the limitations they impose on the provability of necessity, as well as the legality, proportionality, transparency, and the possibility of review they provide to AI governance.

2.1 Early Surveillance Jurisprudence

The Kharak Singh v. State of Uttar Pradesh case is important more for the constitutional constraints it reveals than its factual narrative [7]. The majority decision deemed domiciliary visits to be unconstitutional as it involved the police gaining entry to a person's home after dark and would, therefore, affect personal liberty. However, the majority decision left intact the police practice of shadowing and other forms of surveillance. In this instance, the majority decision privileged visible physical intrusions to the police practice of maintaining a register and constant physical observation of the subject. In the context of inference and infrastructure, this decision restrained the collection of one type of surveillance, but did not challenge the predictive classification of a subject as a security risk [8]. The dissenting opinion was more appropriate, as it considered privacy part of the personal liberty of the subject, as well as the cumulative effect of the surveillance regime. This decision is therefore doctrinally deficient, as the constitutional protection was afforded to the place of intrusion, and not to the state's infinitely extensible and operational power to construct and implement a classification of surveillance of a subject, who is presumed to possess the propensity to engage in criminal activities, without providing the subject notice, an explanation, or a means to contest this classification.

The case of Govind v. State of Madhya Pradesh advanced the doctrine of privacy by arguing that the police's prolonged surveillance was capable of impacting an individual's liberty, movement, and right to association, and even to the sanctity of a person's private life [9]. The case was a landmark in that it argued that the right to privacy may be violated even in cases where the police do not make a physical intrusion into the premises. However, the case's argument that the police may be within their right to exercise surveillance if it is in the case of a compelling state interest and if it is a matter of the executive's reasoned judgment is a drawback. The case was silent on independent authorization, notification, and the remedy to correct the suspicion that was stored. Using the inference framework, this is a significant omission as surveillance is not a passive observation of behavior. The case laid down an implicit requirement for limitation and the temporal restraint of surveillance, but left the individuals outside the framework that determined and imposed risk [10].

2.2 Informational Privacy and Publication

R. Rajagopal v. State of Tamil Nadu expanded the concept of privacy from hindrances caused by physical trespassing to the control over the release of one's private information [11]. The court defended unpublished private information; however, it denied sweeping prior restraints on the publication of information related to public records and the actions of public officials. While important to press freedoms, the aforementioned distinction is inadequate for systems based on inference. Given public information, AI can draw disturbing or reputational conclusions, combine information released for different purposes, and create a narrative that is not directly stated by any of the sources. Thus, the privacy harm may stem from contextual recombination and false attribution, as opposed to the release of a once private fact. While Rajagopal protects from the unauthorized release of private information, the exception for public records does not provide an authorization for uncontrolled surreptitious observation [12]. The contemporary safeguard against inference made from public information should be analyzed in terms of intent, precision, context, and the impact that inferences are likely to have.

2.3 Privacy as a Fundamental Right

Justice K. S. Puttaswamy (Retd.) v [13]. Union of India lays down the foundational principles for regulating inferencing systems. The nine-judge Bench located privacy not within the limits of secrecy or the home, but rather within dignity, autonomy, bodily integrity, control over one's information, and freedom to make one's own choices. Their framework of legality and proportionality subjects to scrutiny systems that collect vast amounts of data, make predictions,

and control access to public or private resources. This decision also recognizes the positive obligation to defend individuals from the onslaught of technology, and is applicable here, where private entities practice quasi-governance and control through scoring, moderation, or synthetic attribution. What Puttaswamy does not provide is operational [14]. Inferred rights in Puttaswamy do not establish the right to be notified of automated processing, to have access to attributes, to receive substantial justification, or to have human correction of probabilistic judgments. Consequently, within the context of Puttaswamy, it is necessary to execute and implement laws and policies within specific sectors so that a person aggrieved by a decision of great consequence can bring forth a valid challenge against such a decision.

2.4 Aadhaar and State Data Infrastructures

K. S. Puttaswamy (Aadhaar) v [16]. Union of India reveals both strengths and weaknesses of purpose-based assessment of data structures. The Court defended Aadhaar for welfare-related verifications while barring forms of private and commercial uses that went beyond the Act. The Court appears to understand that a system validated for identification and facilitation of benefits may, from a constitutional perspective, be justified for different purposes in different domains. Biometric data is only one element in the risk of inferences. Authentication can lead to inferences regarding the nature, location, and time of services, relationships, and legal entitlements if data is retained or if institutions correlate data [17]. It can be argued that the judgment supports purpose dispensation and function creep, but it can be said to provide little direction on auditing latent functions. A more rigorous interpretation of function creep would posit that each secondary purpose of data must be legally authorized, justified, and bounded technically and in time, and that it would be subject to independent oversight and control.

2.5 Internet Restrictions and Surveillance Oversight

Anuradha Bhasin v. Union of India offers insight into inference governance by treating aspects of publication, temporariness, reasoning, and periodic review as necessary safeguards of transparency against arbitrary executive power [18]. While orders for the suspension of internet access inhibit the exercise of trade and free expression, they also affect individuals' ability to verify official statements, record and substantiate incidents, and refute official accounts of state-generated risks. The Court's position that restricting orders be reasoned, published, temporally defined, and subject to review may also be applied to algorithmic classification systems that determine persons and places as risks. The prediction of a threat that would subsequently invoke surveillance, exclusion, or the restriction of communication should not

remain a privileged and unexamined artifact of a secret and closed technical system [19]. Although the decision does not provide a direct framework for the governance of artificial intelligence, it does provide a more broadly applicable framework of governance; inference-based state action must be identifiable and justifiable to the public in order to challenge the inference-based actions of the state that are implemented as temporary measures.

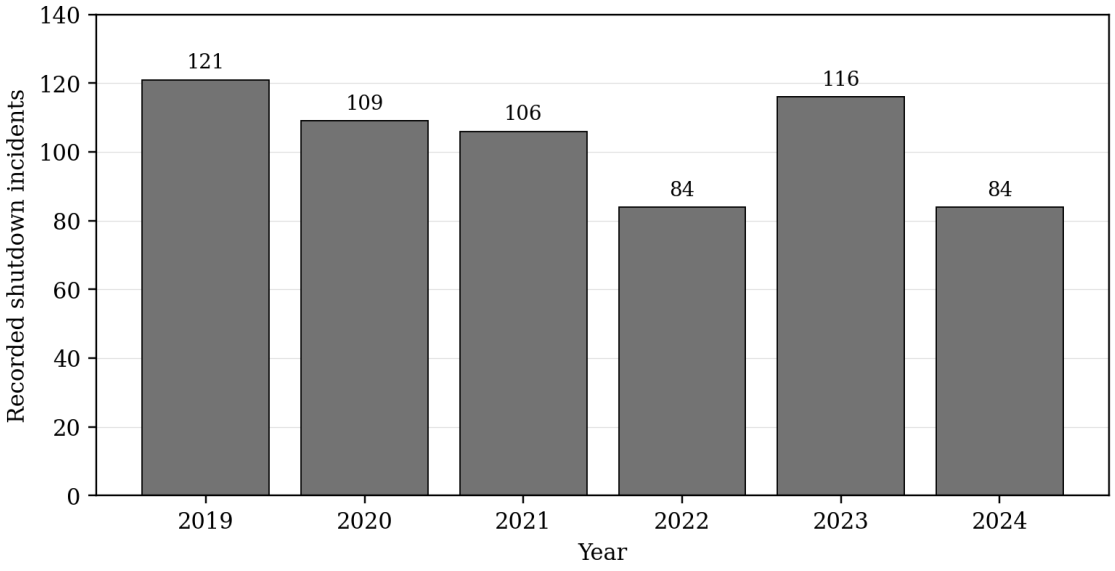

Figure 1. Recorded internet shutdowns in India, 2019-2024. The fluctuation demonstrates that communication restrictions remain a recurring governance instrument whose opacity can obstruct the contestation of inference-based state action.[20], [21]

3. AI AS "INFERENCE INFRASTRUCTURE"

Artificial intelligence is important to the law when it makes the iterative decision-making process a reality with the establishment of a continuous loop of collection, aggregation, modeling, scoring, and acting. The term inference infrastructure describes this process and focuses on the stage in the process when a prediction is recognized as a governing fact. In the context of surveillance, communications metadata and traces of interaction on platforms may be used to score suspicion and draw association maps. In the context of markets, behavioral proxies may influence credit, employment, insurance, or access to a given platform. In the context of generative systems, probabilistic modeling may generate a face, a voice, or a story in such a way that the audience perceives it as real. Current Indian law has some provisions for this process in the context of interception authorizations, the duties of intermediaries, directives on cybersecurity, biometric law, and laws on the protection of personal data [22] [23]. The main gap in the law is that these provisions are mainly focused on access to data, the transfer of data,

the retention of data, or the removal of data, whereas the main legal damage occurs when the derived decision is implemented against a specific target.

3.1 What Is an Inference

An inference is a statement about a specified individual that is generated from data that is observed or collected about them, as opposed to data that is provided about them. Information such as a purchase history, timestamp, and identifier, in conjunction with a person's biometric data and interaction with a platform, can be used to formulate statements about a person's health, political preferences, trustworthiness, risk of committing fraud, employability, and behavior. These statements assume a legal effect if the statements are used to make a determination, regardless of the fact that the statements are referred to as analytics or internal scores by the company. Under the Digital Personal Data Protection Act, 2023, statements about a person can be made if the person is identifiable [24]. Processing, notice, consent, and other rights are provided in the Act. A legal right to contest a statement may exist, but a person has no means to contest an adverse outcome or correct an inaccurate statement if the inferred attribute and the responsible party are not disclosed in an intelligible manner.

3.2 Profiling and Automated Decision-Making

Profiling makes differentiation tangible by assigning individuals to categories that determine their risk, value, trust, or eligibility. Profiling's privacy impact is different from standard data collection. Individuals may be managed based on traits that they never articulated or even know exist [25]. The DPDP Act provides indirect control over lawful processing, consent, and legitimate/fiduciary uses, and it provides access, correction, and grievance mechanisms. It does not provide for a general right that can be compared to Article 22 of the GDPR, the right not to be subject to decisions taken as a result of automated processing. Therefore, formal consent can be given to invasive profiling in the context of broad, bundled, and undisclosed notice [26]. The Information Technology Rules provide for privacy protection against invasion, deceptive attribution, and impersonation at the content layer, but they do not provide for a general right to contest a hidden risk model. An inference-focused approach requires significant notice of profiling, disclosure of material attributes, and reasoned human review with a right to appeal.

3.3 Technical Risks

The absence of raw-data provision during the execution of machine-learning models does not indicate harm is absent. Attacks on inversion models could re-create sensitive data or equivalent instances [27], [28]. Attacks that infer membership could determine if an

individual's data was part of the training data. The generative systems pose an analogous evidence risk (even more pronounced and dangerous) by producing a synthesized face, voice, or behavior that could be accepted as authentic evidence. These injuries occur from the model's architecture and training, from the control of the output, from the Access provision, not from database theft [29]. Section 8 of the DPDP Act could help understand the necessity of security provisions more clearly, but the Act's requirements will include testing the extraction, the output's control, the rate and log of the access, the assessment of the red-team, and the incident response to model leakage. The duties of the intermediaries concerning privacy and impersonation and the misleading content will deal with the circulation after creation, while the governance of the model will help reduce the first inference harm and the extent of that harm.

3.4 Conceptual Framework for India

The constitutional test of legality, legitimate aim, necessity, and proportionality is an effective framework for evaluating inference pipelines in India [30]. Regarding legality, the relevant collection, derivation, and operational use must be grounded in formal legislation. Regarding legitimate aim, sufficient precision in stating the purpose must be provided by the state or fiduciary. About necessity, there must be consideration of the means used and limits imposed that are the least intrusive in regard to data fields, model features, retention, and reuse. Regarding proportionality, the potential benefits must be weighed against the risk of error, the likelihood of discrimination, the chilling effect, and irreversible harm to the individual's reputation or identity. Safeguards must be maintained and include records of authorization and review as well as access controls, audit trails, and correction mechanisms [31]. This proposed test enables the DPDP Act and interception law to be read in conjunction with the intermediary rules and sectoral regulations, with a focus on the individual impacted by the inference rather than on the organization that retains the source data.

4. INDIAN STATUTES AND EXECUTIVE FRAMEWORKS THAT ENABLE OR CONSTRAIN INFERENCE

The law in India provides for inference through a fragmented patchwork of legal instruments for interception, cybersecurity, data protection, and biometrics, and other sector-specific frameworks [32]. The Digital Personal Data Protection Act, 2023, and related other frameworks prescribe the limits of data capture, storage, dissemination, and erasure; however, they do not address the complete process of how raw data morphs into identity, intent, credit,

employability, or risk measurements. The problem is of a structural nature. The law allows data to be collected for security and identification or the provision of a service, and the data may later be used, without a separate test of necessity and proportionality, for a purpose significantly different from that for which the data was originally collected. The following analysis uses the inference paradigms for each of the above-mentioned laws to examine the extent to which they provide for limits on secondary use, attributes, inference automation, error remediation, and self-regulation [33]. The answers to these questions will show whether the right to privacy is protected at a constitutional level, or at the operational level, or whether the right to privacy is restricted solely to the first instance of data collection.

4.1 State Interception and Monitoring

Section 5(2) of the Indian Telegraph Act, 1885 and Section 69 of the IT Act, 2000 respectively permit the interception and monitoring of communications [34]. For both acts, interception and monitoring are subject to the rule of law and formal procedures. Safeguards for both acts include the approval of a competent authority, documented reasons, and an executive review. Both systems constrain access to communications, but neither of them sufficiently addresses the analytics performed after access. There are numerous examples, including the construction of social graphs, association scores, location patterns, and threat classifications regarding the decisions that will be made in the future, that will be based upon the analysis of intercepted communications and metadata [35]. The extent of executive review is also limited, as the same authority both approves and reviews the action. The Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024 provide for a lawful interception system, but an inference-based system would require the logging of system queries, restrictions on system training, deletion of non-relevant results, and a documented review of the error rate. Negative actions that result from the use of an automated system and that are based on an adverse outcome would also be required to be reviewed.

Law[36]	**Grounds[37]**	**Procedure**	**Oversight**	**Case-law touchpoints**
"Section 5(2) of the Indian Telegraph Act, 1885" read with interception	Public emergency or public safety; necessity or expediency for sovereignty and	Written order by competent authority; reasons recorded; procedural	Executive review committee structure and periodic	"*People's Union for Civil Liberties v. Union of India[39]*, ";

Law[36]	Grounds[37]	Procedure	Oversight	Case-law touchpoints
safeguards under Telegraph-rule architecture, now addressed through telecom interception rules in 2024	integrity of India, security of the State, friendly relations with foreign States, public order, or preventing incitement; reasons recorded in writing	documentation and retention; telecom interception rules specify defined roles for entities and review structures[38]	review; compliance reporting within the executive chain	"*Justice K.S. Puttaswamy (Retd.) v. Union of India[40]*, "
"Section 69 of the Information Technology Act, 2000" with the "Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009"	Statutory grounds for directions; alignment with national security, public order, and related interests through the enabling provision and rules-based thresholding	No interception, monitoring, or decryption without competent-authority order; procedural safeguards in the 2009 Rules govern issuance, handling, and record management	Review committee reference and structured oversight within the rule's architecture.	"*Justice K.S. Puttaswamy (Retd.) v. Union of India[41]*, "

Table 1. Legal bases and safeguards governing interception in India.

4.2 Digital Personal Data Protection Act, 2023 and DPDP Rules, 2025

The Digital Personal Data Protection Act, 2023 is the first comprehensive framework for data protection that can extend to inferred data in a given jurisdiction, as it governs the processing of data of identifiable persons and prescribes obligations on Data Fiduciaries [42]. The profiling, outputs of the models, and the obligations of Significant Data Fiduciaries would be governed by the clauses relating to purpose limitation, accuracy of data, safety measures, and safeguards, and provisions pertaining to erasure, redress of grievances, and obligations of

Significant Data Fiduciaries. This Act has three principal gaps. It does not say that inferred attributes and scoring constitute personal data. The right to access may be interpreted as the right to see the source data, rather than the right to see the inference. Finally, there is no right to demand an explanation or a right to a review by a person of a decision that was entirely made by a computer [43]. The Digital Personal Data Protection Rules, 2025 bring some structure to notification, consent, management, data related to minors, breaches, and grievance reporting. However, these Rules do not impact the standing and the ability to challenge high-impact inferences.

DPDP duty focus[44]	**Statutory or rules hook**	**What it constrains in practice**	**Profiling or inference risk addressed**	**Residual risk in high-inference systems**
Purpose limitation	"Digital Personal Data Protection Act, 2023" duties framework for lawful processing tied to specified purpose and notice-consent design	Repurposing collected identifiers into new prediction tasks without fresh legal basis	Silent function creep from service delivery into behavioural scoring	Broad purpose drafting and bundled consent can still permit expansive inference
Data minimisation and necessity	Act-level duty set that ties processing to necessity for the specified purpose.	Excessive field collection and persistent telemetry capture	Overfitting of profiles from rich traces and cross-context correlation	Data that appears "necessary" for security or fraud screening can still enable intrusive models
Storage limitation and erasure	Act rights to correction and erasure; duties limiting retention beyond purpose; operationalisation	Indefinite retention of raw logs and derived scores	Long-horizon risk scores that outlive context, amplifying stigma	Models trained on historical data may preserve inference even after deletion of source records

DPDP duty focus[44]	Statutory or rules hook	What it constrains in practice	Profiling or inference risk addressed	Residual risk in high-inference systems
	through notified rules structure			
Transparency through notice and access	Act notice and access rights; rules-style scaffolding for how notices and requests function	Hidden profiling and opaque attribute generation	Individuals remain unaware of sensitive inferences such as health, sexuality, or politics drawn from proxies.	Notice can stay high-level, leaving model features and correlation logic undisclosed.
Grievance redress	Act grievance right and fiduciary obligation to provide redress pathways	Lack of internal review of harmful automated outputs	Unchecked automated denials in welfare, finance, or content takedowns	No dedicated right against solely automated decisions like "Article 22 of Regulation (EU) 2016/679"[45]

Table 2. DPDP Act duties and residual inference risks.

4.3 CERT-In Directions, 2022

According to the CERT-In Directions 2022, agencies are required to maintain system logs and synchronize system clocks [46]. Agencies also must report specific cyber incidents and provide requisite information to assist with cyber incident response. These Directions promote legitimate purposes for protecting the cybersecurity of systems and networks. However, system logs and records have the potential to be used for linkage and reasoning tasks as they persistently record information for personal device identification, user behavioral evaluation, and risk scoring. There is an inference problem when security logs are general organizational resources and are subsequently used for moderation, fraud detection, employment surveillance, and even for law enforcement purposes, in the absence of a legal framework that justifies those

purposes [47]. Therefore, logs should be isolated from other resources, and access to logs should be controlled and logged. Additionally, the authorization for log usage should be formalized, and the disposal of logs should be verified by a third party. In the absence of these provisions, the purpose of logs may be extended from incident response to continuous surveillance depending on the provisions required for compliance.

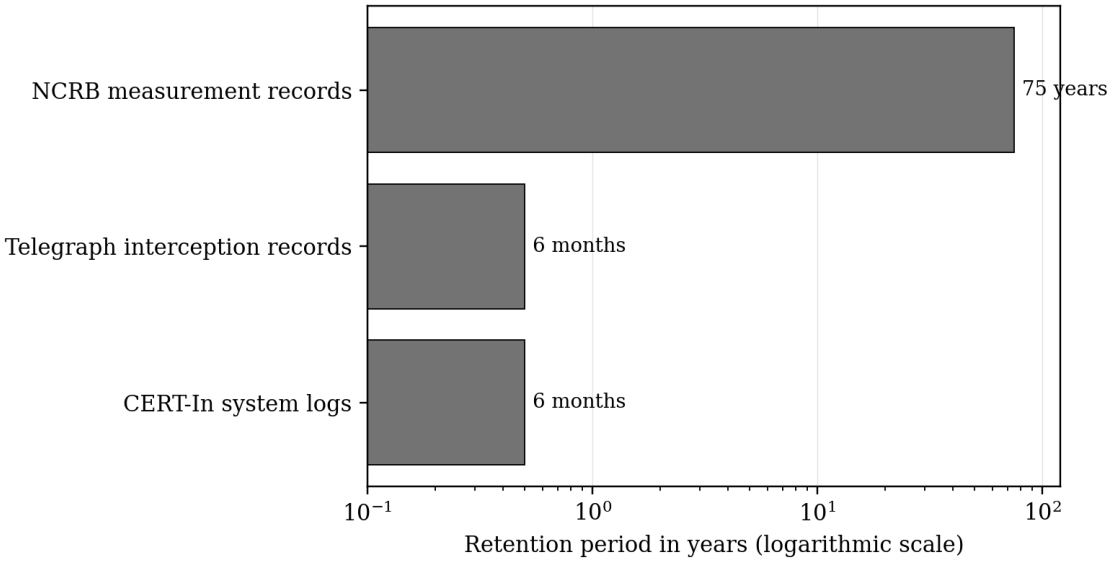

Figure 2. Selected statutory retention periods relevant to downstream inference, shown on a logarithmic scale. The comparison demonstrates how short-term security logs and long-term biometric records create materially different capacities for correlation and reuse.[38], [43], [48]

4.4 IT Rules, 2021 and Deepfake Policy Measures

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (hereafter "IT Rules") require intermediaries to set up notice, grievance, and content-response systems. In practice, compliance with the IT Rules has become reliant on automation of detection, classification, ranking, and profiling of a given account. The governance mechanism therefore infers harm while trying to mitigate and control the dissemination of harmful content. The Ministry of Electronics and Information Technology (MeitY) advisories on deep fakes, and the proposals for the 2025 Draft on Synthetically Generated Information, are moving towards the implementation of provenance with the use of labels, metadata, user statements, and corroborative technologies [48]. While these may increase recognizability, they do not mean that labeled content is not harmful, that unlabelled content is false, or that an automated detection result is correct. A justifiable system must have evidence, retention, notice,

justified removal, and grievance mechanisms for the misclassification of lawful content [49]. Provenance is a useful system only when paired with accountability for the inferences drawn from the suppression of content.

4.5 Criminal Procedure (Identification) Act, 2022

The Criminal Procedure (Identification) Act, 2022 has provisions for the enhancement of collection of physical, biological, and behavioral measurements and their long-term management within the National Crime Records Bureau (NCRB) [50]. It has major implications for the inference infrastructure as it has the potential to create a reusable repository of measurements, as compared to the continuum of measurement. A biometric template collected for one purpose can potentially be a key to a database for future searches across different databases, different surveillance systems, and different investigations. The long-term retention of the template increases the potential for cross-case linkage, construction of watch-lists, and inference of various entities. The deletion mechanisms are limited, and the oversight system of the Act is primarily within the Criminal Justice System itself [51]. The Act also does not develop a system through which the affected individuals can access the system to see a match, contest a false positive, or ascertain if a secondary use of the system maintained its primary purpose. A review of the constitution must, therefore, look at retention, reuse, accuracy, access, and implications of a match, and not just the initial collection of the sample.

Measurement type	**Purpose**	**Retention**	**Oversight**
Fingerprints, palm and footprint impressions, photographs, signature and handwriting	Identification, investigation support, and record management within criminal justice functions	Long-term retention through NCRB-managed records with deletion only within defined statutory pathways	Statutory structuring through authorised collection and NCRB custody, with legality contestation routed through constitutional review rather than a dedicated privacy regulator
Iris or retina scans and other biometric traits[51]	Biometric anchoring of identity to enable matching and search across datasets	Long-term retention that supports repeated future matching	Oversight primarily internal to the criminal justice chain, with limited transparency to the affected person absent separate disclosure duties

Measurement type	Purpose	Retention	Oversight
Biological samples and analysis	Forensic and identity support functions that can extend into attribute inference depending on analytic methods	Long retention increases risk of secondary use and cross-case linking	Safeguards depend on lawful purpose framing and procedural discipline rather than explicit limits on derived inferences

Table 3. Measurements, retention, and safeguards under the Criminal Procedure (Identification) Act, 2022.

4.6 Sectoral Uses of Facial Recognition

Facial recognition epitomizes the phenomenon of function creep in inference infrastructure [52], [53], [54]. The same matching capability that began with the identification of missing persons can now be seen being applied to access control, crowd management, verification of entitlement to welfare, and general policing. Increased National procurement activity coupled with the reported deployments in Delhi and Telangana suggests a rapidly growing capability to search across multiple image repositories and feeds of the public domain. The legal risk extends beyond the collection of biometric data. Systems that generate identity assertions may operate with watchlists, varying quality of images, and the subjective interpretation of operators [55]. These systems will inevitably produce false positives and can be designed to produce asymmetric and unequal error. In the absence of a statute, independent oversight, and established measures of accuracy, legal proportionality is hard to sustain. In such cases, the legal framework ought to mandate specific watchlists, the prior technical assessment of the systems, human verification, and public reporting of the mechanisms and legal redress. Continuous scanning of the public may be authorized only under exceptional circumstances and only for a limited time by a court of law.

5. GENERATIVE AI, DEEPFAKES, AND PERSONALITY RIGHTS AS PRIVACY

Systems that are generative obfuscate privacy by transmuting it into a matter of attribution, identity, and the reliability of evidence. Any output produced synthetically may lead an audience to conclude that an individual either verbally or non-verbally expressed or conferred consent to actions that never transpired. Thus, there is injury not only to truth, but also to the appropriation of identity markers (i.e., facial, vocal, and physical expressions), along with the shifting of the burden to the represented individual to deny the expressed actions [56]. While Indian law addresses some aspects of this injury through its various mechanisms (i.e., intermediary duties [57], defamation, intellectual property, personality rights, data protection,

and injunctive relief), there is no unified system that addresses the entire process of model creation, publication, dissemination, and repurposing. While the judicial arms have focused on the protection of persona and reputation, the executive branches have focused on Labeling and removal. The inference-infrastructure framework addresses the attribution of falsehoods, safeguards and prevents evidence, and addresses the removal of multiple uploads, and is applicable to rights of claimants that are not well known.

5.1 Advisories and Draft Amendments

Since 2023, MeitY has classified deepfakes primarily as an intermediary due diligence issue. This approach ignores the statutory classification of deepfakes as an inference harm [58]. The advisory in March 2024 called for swift action to curb illegal synthetic media. On the other hand, the October 2025 draft proposals included a definition of synthetic media and included the concepts of Labeling, embedded metadata, user statements, and a verification system. This model is sound because the venues for publication and distribution are under the control of the respective platforms, but it is of limited scope because of the reliance on private detection systems and rapid content adjudication. Labeling proves the content a system has classified as a deepfake, but it does not address the issue of consent, the reputational harm, and the ill-effects of the erroneous classification. In order to achieve a complete due diligence system, there has to be an obligation to enforce standards for the creators and the users of the systems, the preservation of disputed content, and authenticated requests for removal, along with the provision of transparent and adjustable confidence levels regarding the classification and a system to counter both under-removal and wrongful removal of classified content.

5.2 Recent Indian Case Law on AI Misuse and Personality Rights

Amitabh Bachchan v. Rajat Nagi & Ors. shows both the advantages and challenges of personality-rights injunctions within an inference-based framework [59]. The Delhi High Court prohibited the unauthorized commercial usage of the claimant's name and likeness in regard to indicia in changing online and offline media. This remedy is designed to respond to the iterative nature of digital infringement and recognizes that the remedy may be inadequate if restricted to a single file or known defendant. This remedy's doctrinal reach is still narrower than the privacy concerns articulated in this article. Personality rights are most readily enforced where identity has established commercial value and synthetic attribution may inflict harm on any individual through damaging effects personally, professionally, politically, and socially. Thus, this order should be interpreted as a rapid corrective, stopgap model [60]. The absence of

privacy in the contemporary digital context continues to necessitate a framework pertaining to the right to control consent and the attribution of identity for a claim to be made by individuals beyond the celebrity class.

Anil Kapoor v. Simply Life India & Ors. builds a foundation for the legal protection of a multitude of identity elements in the digital realm, including name, image, and voice [61]. Generative AI cannot appropriate identity by creating a copy of a protected work in the traditional sense. This case understands that a model could create an endorsement in a person's voice or mannerisms, allowing the model to disseminate statements and endorsements that may be false to the public before the standard post-publication remedies would take effect. The interim order seeks to remedy the speed and irreversibility of the harm [62]. This case does not set the threshold for over-removal of legitimate parody, nor does it preserve evidence. The decision reinforces that synthetic likeness does infringe privacy, and that the protection of the privacy of one's synthetic likeness does outweigh the right to freedom of expression.

The proceedings recorded in Abhishek Bachchan v. Various Websites have to do with AI-generated identity manipulations and uses, and demonstrate why dynamic relief is essential in online personality cases [63]. The relevant injury is attributional. The publication of a new URL or altered file leads to a renewed inference that the person actually produced, approved, or engaged with the content. There is a need for a more rapid or dynamic mechanism, matched with preserved copies and a way to contest erroneous designations. In the absence of such mechanisms, a more rapid or dynamic mechanism would lead to the same automated tools being utilized to detect reuploads being used to suppress lawful commentary. This case demonstrates the need for rapid containment of identity-based synthetic harm, and the need for a transparent evidentiary protocol in relation to the contested output, identity, and the relief being requested.

In Aishwarya Rai Bachchan v. Aishwaryaworld.com & Ors., the case's interim protective order demonstrates that the courts recognize the unauthorized use of an individual's name or image online can result in real, ongoing reputational loss and commercially adverse effects. Though private endorsement and celebrity promotion are a narrower use case. Generative media and AI tools are able to create an infinitely iterative and more convincing answer than any correction. An order may limit some aspects of the injury, but most of the working solutions would have to be named and addressed in a comprehensive manner to include removal of search results, notice, and protections against essentially the same uploads. Because it is

dependent upon the intermediary, the same is true of personality protections. Ultimately, user-generated content needs to be treated differently than legitimate reporting and parody. The burden of proof and the answer should not be left to private actors' or intermediaries' discretion.

The interim relief granted to Shilpa Shetty Kundra in Shilpa Shetty Kundra v. Getoutlive In & Ors. is tracking the same emerging pattern as several Courts where unauthorized usage of personality traits leading to the digital dissemination of information that can result in permanent reputational harm is at issue. These Courts have noted the relevance of the "inference-infrastructure" theory. The relaying of information repeatedly can result in irreversible reputational harm. Injunctions, as well as takedown orders, are necessary to address the initial harm, but they are reactive and rely on the cooperation of digital intermediaries. The primary concern is for the unrepresented individual, as both injunctions and takedown orders require that individual to have the means to access the Courts on an urgent basis. As for the unrepresented individual, privacy protections will remain ineffective. It is important that digital intermediaries implement rapid, cost-efficient features that protect privacy against unauthorized use of personality traits, and that the Courts provide adequate protections without regard to the commercial viability of the particular case.

5.3 Remedies and Safe Harbour

The combination of deepfake remedies and personality-rights remedies includes injunctions, platform takedowns, grievance redressal mechanisms, and the conditional safe harbour under Section 79 of the Information Technology Act, 2000 [64]. The main challenge in dealing with deepfakes is the balance between the adverse effects of delay and the adverse effects of rapid response. The damage caused by deepfakes may become irreversible. On the other hand, a rapid response may remove lawful speech and evidence necessary for adjudication. A response framework should stipulate a validated notice announcing the protected attribute, the false attribution, and the precise or substantially identical content [65]. The preserved content should be accompanied by a disposal rationale, a removal rationale, a reupload mechanism, and a reupload-review mechanism. Similarly, the response should be dictated by the removal rationale and should be precisely framed, allowing for extensions to new representations with a similar objective. These mechanisms will combine privacy and relief from deepfakes with protected compliance from safe-harbour provisions.

5.4 IndiaAI Mission and Compute Infrastructure

The IndiaAI Mission analyzes the placement of computational infrastructure within the legality framework at large [66]. The opportunity to build and deploy high-impact AI systems is a function of large-scale training and inference resources. Therefore, state-sponsored computation is, by definition, not a neutral subsidy. It can be "configured" to condition the provenance of data, documented legal justification for personal data, records of reproducible research, model-security assessments, audits, incident reporting, and retention and deletion of intermediate artifacts. Shared infrastructure can enable research to address issues of bias, extraction, membership inference, and the generation of synthetic media. It is favourable to assert obligations at the computation and procurement phases, rather than relying solely on post-deployment obligations, as it provides leverage against the deployment of harmful models at large. The primary question of governance is whether publicly funded resources will only enhance inference capability, or whether they will create legally binding and technically enforceable conditions to audit the downstream processes of AI and the generation of personal identities.

Dimension	**India (DPDP plus IT regime and related directions)**	**EU (GDPR Article 22 and EU AI Act)**
Core right against harmful automated decisions	No general right equivalent to "Article 22 of Regulation (EU) 2016/679"; protection relies on DPDP duties, sectoral rules, and constitutional review	"Article 22 of Regulation (EU) 2016/679" provides a structured framework for decisions based solely on automated processing with legal or similarly significant effects, coupled with safeguards described in EDPB-endorsed guidance.
Governance of synthetic media and labelling[67]	IT Rules due diligence plus MeitY advisories; 2025 draft amendments propose mandatory labelling, metadata embedding, and user declarations with technical verification.	EU AI Act introduces transparency duties for certain AI uses and a tiered risk framework; timeline and obligations are anchored in Regulation (EU) 2024/1689 and Commission timeline communications.

Dimension	India (DPDP plus IT regime and related directions)	EU (GDPR Article 22 and EU AI Act)
Prohibited practices and high-risk controls	Sectoral and general-law constraints without a single AI risk statute; interception and biometrics governed through separate laws and directions	EU AI Act establishes prohibited practices and high-risk obligations, with phased application points and institution-building such as the AI Office.
Remedies and enforcement levers	Injunction and takedown-centred remedies for persona harms; platform compliance through IT Rules; DPDP enforcement through Board structure and duties framework	Supervisory authority enforcement under GDPR plus AI Act enforcement mechanisms; phased start for general-purpose model obligations in 2025 and later high-risk timing in Commission-confirmed schedule

Table 4. Comparative safeguards for inference and automated decision-making in India and the European Union.

6. DOCTRINAL AND INSTITUTIONAL CHALLENGES

6.1 Doctrinal Coverage and Contestability

The first issue is with the doctrine coverage in Indian law. Indian law is silent on when a score, prediction, similarity match, or synthetic representation is personal data or a legally reviewable determination. Undoubtedly, there are access and correction limitations-the access and correction rights may be limited to the source documents. If the determination is in part based on undisclosed reasoning, the person may have no means to challenge the determination. The right to proportionality provides a standard that is constitutional, yet in practice, the right may not be invoked in time to remedy a harm that has already been caused. This right would not reach the private sector with the speed necessary to address the routine and frequent violations that affect the people [68]. The lack of a general right to be informed, to receive an explanation, to access a determination, and to appeal the decision leaves the person in the absence of a means to contest the determination. Contestability of a decision or determination should be considered a substantive component of a right to privacy rather than a means to contest an arbitrary decision.

6.2 Institutional Fragmentation and Oversight

The second obstacle is institutional fragmentation. Different Acts and different purposes and structures for oversight cause fragmentation among telecommunications authorities, CERT-In, law enforcement, intermediaries, sector regulators, and the Data Protection Board. Due to various data sharing, procurement, platform requesting, and secondary analytics practices, there is no agency that will review the entire process. Executive review committees will look at the authorization, if at all, while sectoral regulators will look at compliance of the service without access to the model design and training data. When systems merge public and private data or create cross-sectoral impacts, as the case may be, a unified oversight mechanism is necessary. Shared audit requirements and referral mechanisms coupled with the responsibility for cross-system impact would mean that the de facto inference would not be outside the jurisdiction of any of the authorities [69], [70], [71].

6.3 Technical Opacity and Evidentiary Harm

The third challenge addresses technical opacity and the burden to prove. Organizations may withhold outputs, feature importance, and training data under the guise of confidentiality. However, affected parties are expected to prove something that they cannot even inspect. In addition, outputs from probabilistic models are not necessarily the same, and generative models can eliminate the difference between what is real and what is fake [72], [73]. The privacy risks of model inversion, membership inference, and model data extraction illustrate that privacy harm can happen in the absence of a direct disclosure of information. The law must guarantee the preservation of models and logs, access to these models and logs by independent experts under confidentiality protection, and the disclosure of material factors of a decision, while assigning the burden of proof to the actor in possession of the relevant evidence. In the absence of these provisions, the technical intricacies of the models create a de facto immunity from judicial correction and control.

6.4 Remedial Inequality and Access

The fourth challenge is remedial inequality. Emerging personality-rights cases show that identity-based synthetic harm can be addressed with urgent injunctions. Still, most people lack the means to go through the process of identifying the defendant, collecting and preserving evidence, obtaining the required technical support, and then going to a constitutional court or commercial court. There are many frustrations with the speed and transparency of platform grievance systems. There can be failures in automated removal systems with respect to harmful

copies and even suppressing lawful material. Repair systems should be grounded in non-monetary, non-legal defensive status systems. Remedies should, among other things, eliminate the infrastructural inequalities of informal burdens (i.e., loss of funding and legal aid) and create an obligation to take action and remedy the violations [74], [75]. The inequalities of repair systems must be addressed to make inference rights enforceable. Repair systems grounded in equality are a constitutional concern. Uncorrected false inferences can affect someone's job, their standing with the law, their reputation, their family, and even their credit.

7. CONCLUSION

The article contends that Indian privacy law must also incorporate the production and use of inferences. Laws and frameworks must adopt a proactive approach to the prevention of significant privacy-related injuries that result from profiling. In addition to the aforementioned, we also have to consider the use of facial recognition, artificial intelligence (AI)-generated technologies, and the use of other technologies that transform multiple, dispersed data points into judgments about a person's risk, identity, trust/or lack of, entitlement, and reputation [76]. Puttaswamy provides a constitutional grounding of dignity, autonomy, and legality along with the proportionality test. The DPDP Act may provide duties and rights that may be construed to extend to implied rights, protections, and attributes [77]. However, the statutory framework is inadequate. The principal finding is that the existing legal frameworks provide privacy protection in areas that are no longer relevant, whereas the greatest privacy protection is required in areas that are currently unregulated.

An inference framework will be legally robust if it lists the basis for its formation and rationale for its use, its aims, if it's designed in a proportional manner, if its results are precise and can be assessed, and if it provides a remedy for the decisions it has most influenced. There should be access to and the ability to amend significant inferred data; the obligation to safeguard should also apply to the extraction and leaking of a model, and high-significance automated decisions should be accompanied by a right to know, justification, human oversight, and the right to appeal [78]. Most of these can be sought through the DPDP Act, accompanying sectoral rules, Conditions of Contract pertaining to procurement, and Constitutional review. However, there are limits to the breadth of interpretation. The more certain area of statutory law will reduce reliance on piecemeal litigation [79]. The main argument of the article is that the person the system has constructed should be visible to the law. The system should regulate the impact

of the organization's knowledge, the methods used to gather that knowledge, and the social or legal consequences of its application.

8. DOCTRINAL AND REGULATORY RECOMMENDATIONS

The following recommendations apply the inference-infrastructure model to legal and administrative frameworks to address the major issues identified in the analysis. These issues include unclear treatment of derived data, lack of a general right to challenge automated decision-making, fragmented oversight, the subsequent use of security and interception data, insufficient control over biometric matching, reactive approaches to deepfake regulation, and limited responsibilities for model security. These measures can all be implemented through some combinations of the DPDP rules, sectoral regulation, conditions of procurement, judicial rules, and legislation. The aim is to relocate contestability and proportionality to the moment when an inference is drawn and put into practice, as opposed to relying almost entirely on corrective measures after an adverse effect has taken place [80].

1. The Central Government should clarify through binding rules or authoritative guidance that a derived attribute, score, classification, or prediction concerning an identifiable individual constitutes personal data when it is stored, communicated, or used to influence a decision.[81] Data Fiduciaries should disclose, on request, the principal inferred attributes associated with the Data Principal, the source categories used to generate them, the purpose of their use, and whether any inference materially affected an outcome. Correction and erasure procedures should extend to inaccurate or obsolete inferences, subject to narrowly defined legal-retention duties. This clarification would connect purpose limitation and access rights to the information that actually governs the person, rather than only to the source records from which it was derived.[82]
2. Indian law should create a right to human review where solely or predominantly automated processing produces legal or similarly significant effects.[83] The minimum procedure should include advance or contemporaneous notice that automation is being used, a statement of the decisive factors in intelligible language, access to relevant inferred attributes, an opportunity to submit corrective material, and review by a person authorised to change the outcome. Sector regulators, including the Reserve Bank of India, the Insurance Regulatory and Development Authority of India, MeitY, and the Ministry of Home Affairs, should incorporate the same guarantees into licensing, supervision, procurement, and grievance standards. A common procedural baseline

would reduce sectoral inconsistency and make constitutional proportionality enforceable in routine administration.[84]

3. Algorithmic Impact Assessments should be mandatory before deployment of high-risk systems in welfare allocation, credit, employment, insurance, biometrics, law enforcement, and essential platform services. The assessment should identify the legal basis, intended purpose, affected groups, training and validation data, accuracy thresholds, foreseeable bias, false-positive and false-negative consequences, human-review arrangements, security risks, and mitigation measures. Significant Data Fiduciaries should obtain independent audits at defined intervals and publish a summary that protects legitimate confidential information without concealing material risks. Deployment should be suspended where testing does not meet sector-specific accuracy or fairness thresholds. This requirement would move oversight from post-harm grievance to documented ex ante justification and continuing review.[85]
4. Logs retained under the CERT-In Directions, 2022 should be technically and organisationally separated from commercial analytics, employee monitoring, advertising, and general user profiling.[86] Access should be limited by role, each query should be recorded, and secondary use should require a separately documented legal basis and purpose assessment. Requests from public authorities should identify the relevant statutory power and be subject to retention and disclosure controls. Entities should publish aggregate information concerning access, preservation, and deletion without exposing security-sensitive details. Independent audit should verify that expiry schedules are enforced and that derived profiles are not preserved after source logs are deleted. These measures would prevent cybersecurity compliance records from becoming a permanent and unreviewed source of behavioural inference.
5. Interception frameworks should regulate analytic use after acquisition, not merely the order authorising access. Agencies should maintain auditable records of every search, correlation, model query, and dissemination involving intercepted material.[87] Non-relevant results and non-matches should be deleted within a defined period, and any adverse administrative or investigative action materially influenced by an automated output should be reviewed by a responsible officer. Review committees should receive information concerning model purpose, accuracy, error, and secondary use, rather than only formal compliance with interception procedure. Aggregate statistics on orders, extensions, data retention, and error should be published in redacted form. This

structure would apply proportionality to the complete inference pipeline and reduce the risk that temporary access becomes indefinite predictive surveillance.

6. Facial-recognition deployment should require a specific statutory or regulatory authorisation that defines the purpose, permitted watchlists, data sources, matching threshold, retention period, and responsible authority.[88] Independent testing should be completed on representative conditions before use and repeated after material system changes. A match should never constitute the sole basis for coercive action, and trained human confirmation should be recorded. Non-matches and incidental captures should be deleted by default. Live crowd scanning should be limited to exceptional, time-bound circumstances approved by a court and followed by public reporting. Individuals affected by a false match should have access to records, correction, and compensation. These conditions would convert a general-purpose identification capability into a legally bounded investigative measure.
7. Deepfake governance should combine interoperable provenance with a rapid and reviewable remedial process.[89] Generative tools and major intermediaries should support visible labels, durable metadata, and authenticated origin records for synthetic audio-visual content, while recognising that provenance does not establish consent or truth. Courts should adopt expedited procedures for identity-based synthetic harm, including preservation orders, verified notices, narrowly framed dynamic injunctions, and directions against materially identical reuploads. Platforms should provide secure interfaces for implementing authenticated orders and should retain an appeal route for lawful reporting, criticism, satire, and parody. Technical detection should be treated as evidentiary assistance rather than conclusive proof. This combined model would address creation, circulation, and remedy without making automated classification the final legal decision.[90]
8. High-risk model developers and deployers should be required to test for training-data extraction, model inversion, membership inference, prompt-based disclosure, and unauthorised replication of identity attributes before release.[91] The test methodology, risk thresholds, mitigation measures, and residual risks should be documented and available to regulators or independent auditors. Controls should include access limits, output filtering where proportionate, rate monitoring, secure fine-tuning, and incident-response procedures. A verified model-leakage event involving identifiable personal data should trigger the relevant breach duties under the DPDP framework even when

no conventional database intrusion has occurred. This approach would treat model behaviour as part of security compliance and would prevent organisations from equating protected storage with protected inference.

9. Access to IndiaAI compute resources, and public procurement opportunities should be conditioned on privacy and accountability requirements that apply before training begins.[92] Applicants should provide dataset provenance records, the legal basis for personal-data processing, documentation of filtering and deduplication, retention schedules, model-security plans, and arrangements for independent audit. Training runs should be reproducible to the extent required for investigation, and intermediate artefacts containing personal data should be subject to defined access and deletion controls. A portion of shared compute should be reserved for accredited researchers testing bias, leakage, robustness, and provenance tools. Public infrastructure would then operate as a regulatory lever that rewards verifiable safeguards rather than merely increasing the scale of inference capacity.
10. An Inference Oversight Sandbox should permit regulated entities to test explanation, review, and contestability methods under the supervision of data-protection and sectoral authorities.[93] The programme should examine counterfactual explanations, feature summaries, model cards, decision notices, human-review workflows, and procedures for correcting derived attributes. Participation should not exempt an entity from existing law, and testing results should be published in aggregated form so that sector-wide minimum standards can be developed. The sandbox should prioritise systems with significant effects and include representatives with legal, technical, and affected-community expertise. Its purpose should be to convert abstract duties of fairness, accuracy, and grievance redress into tested procedural standards that can later be made mandatory through rules, licences, and procurement terms.

BIBLIOGRAPHY

[1] The Digital Personal Data Protection Act, No. 22 of 2023 (India).

[2] Bhatia, G. (2014). State surveillance and the right to privacy in India: A constitutional biography. *National Law School of India Review, 26*(2), 127–147.

[3] Government of India, Ministry of Electronics and Information Technology. (2021). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*. Retrieved January 10, 2026, from https://mib.gov.in/sites/default/files/2024-02/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf

[4] Singh, S. S. (2011). Privacy and data protection in India: A critical assessment. *Journal of the Indian Law Institute, 53*, 663–677.

[5] Government of India. (2025). *Draft Digital Personal Data Protection Rules, 2025*. Retrieved January 7, 2026, from https://innovateindia.mygov.in/dpdp-rules-2025/

[6] Government of India, Ministry of Electronics and Information Technology. (2025). *Digital Personal Data Protection Rules, 2025*. Retrieved January 8, 2026, from https://www.meity.gov.in/documents/act-and-policies/digital-personal-data-protection-rules-2025-gDOxUjMtQWa?pageTitle=Digital-Personal-Data-Protection-Rules-2025

[7] *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295 (India).

[8] *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295 (India). Retrieved January 9, 2026, from https://indiankanoon.org/doc/619152/

[9] *Govind v. State of Madhya Pradesh*, (1975) 2 SCC 148 (India).

[10] *Govind v. State of Madhya Pradesh*, (1975) 2 SCC 148 (India). Retrieved January 8, 2026, from https://indiankanoon.org/doc/436241/

[11] *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632 (India).

[12] *Malak Singh v. State of Punjab & Haryana*, (1981). Retrieved January 7, 2026, from https://indiankanoon.org/doc/501107/

[13] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

[14] *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997). Retrieved January 6, 2026, from https://indiankanoon.org/doc/91938676/

[15] Vengattil, M. (2025, November 14). India strengthens privacy law with new data collection rules. *Reuters*. Retrieved January 6, 2026, from https://www.reuters.com/sustainability/boards-policy-regulation/india-strengthens-privacy-law-with-new-data-collection-rules-2025-11-14/

[16] *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*, (2019) 1 SCC 1 (India).

[17] *Selvi v. State of Karnataka*, (2010). Retrieved January 5, 2026, from https://indiankanoon.org/doc/127517806/

[18] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 (India).

[19] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017). Retrieved January 4, 2026, from https://indiankanoon.org/doc/82461587/

[20] Bhardwaj, S., & Nayak, N. (2020). Rising internet shutdowns in India: A legal analysis. *Indian Journal of Law and Technology, 16*, 122–158.

[21] Bhatia, G. (2014). State surveillance and the right to privacy in India: A constitutional biography. *National Law School of India Review, 26*(2), 127–147.

[22] The Indian Telegraph Act, No. 13 of 1885, § 5 (India).

[23] Russell, S. J., & Norvig, P. (n.d.). *Artificial intelligence: A modern approach* (4th ed.). Retrieved January 4, 2026, from https://aima.cs.berkeley.edu/

[24] Russell, S. J., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.

[25] Padmanabhan, A., & Singh, V. (2019). The Aadhaar verdict and the surveillance challenge. *Indian Journal of Law and Technology, 15*(1), Article 1.

[26] Jauhar, A. (2020). Facing up to the risks of automated facial-recognition technologies in Indian law enforcement. *Indian Journal of Law and Technology, 16*(1), Article 1.

[27] Fredrikson, M., Lantz, E., Jha, S., Lin, S., Page, D., & Ristenpart, T. (2015). Model inversion attacks that exploit confidence information and basic countermeasures. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 1322–1333). Association for Computing Machinery. https://doi.org/10.1145/2810103.2813677

[28] Shokri, R., Stronati, M., Song, C., & Shmatikov, V. (2017). Membership inference attacks against machine learning models. In *2017 IEEE Symposium on Security and Privacy (SP)* (pp. 3–18). IEEE. https://doi.org/10.1109/SP.2017.41

[29] Indian Computer Emergency Response Team (CERT-In). (2022, April 28). *Directions under Sub-Section (6) of Section 70B of the Information Technology Act, 2000*. Retrieved January 2, 2026, from https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

[30] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

[31] Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

[32] Arora-Manohar, D., & Dey, S. (2025). The journalistic exemption under the Digital Personal Data Protection Act: A comparative study. *NUJS Law Review, 18*, 44.

[33] Padmanabhan, A., & Singh, V. (2019). The Aadhaar verdict and the surveillance challenge. *Indian Journal of Law and Technology, 15*(1), Article 1.

[34] Government of India. (2009). *Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009*. Retrieved January 1, 2026, from https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&filename=decryption_of_information_rules_2009.pdf&type=rule

[35] Gazette of India. (2024, August 29). *Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024*. Retrieved January 10, 2026, from https://egazette.gov.in/WriteReadData/2024/256724.pdf

[36] Government of India, Ministry of Electronics and Information Technology. (2021). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*. Retrieved December 31, 2025, from https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf

[37] Bansal, V. (2023, February 13). India's government wants total control of the internet. *Wired*. Retrieved December 30, 2025, from https://www.wired.com/story/indias-government-wants-total-control-of-the-internet

[38] Department of Telecommunications, Government of India. (2024, December 6). *Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024*. Retrieved January 9, 2026, from https://eservices.dot.gov.in/sites/default/files/circular-notifications/procedures-and-safeguards-for-lawful-interception-of-messages-rules-2024.pdf

[39] *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301 (India).

[40] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

[41] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

[42] Sharma, V. (2011). *Information technology law and practice* (1st ed.). Universal Law Publishing.

[43] Indian Computer Emergency Response Team (CERT-In). (2022, April 28). *Directions under Sub-Section (6) of Section 70B of the Information Technology Act, 2000*. Retrieved January 2, 2026, from https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

[44] Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

[45] European Data Protection Board. (n.d.). *Guidelines on automated individual decision-making and profiling for the purposes of Regulation (EU) 2016/679*. Retrieved January 7, 2026, from https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/automated-decision-making-and-profiling_en

[46] Singh, S. S. (2011). Privacy and data protection in India: A critical assessment. *Journal of the Indian Law Institute, 53*, 663–677.

[47] Bhardwaj, S., & Nayak, N. (2020). Rising internet shutdowns in India: A legal analysis. *Indian Journal of Law and Technology, 16*, 122–158.

[48] The Criminal Procedure (Identification) Act, No. 11 of 2022 (India).

[49] Government of India, Ministry of Electronics and Information Technology. (2021). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*. Retrieved January 8, 2026, from https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf

[50] Khera, R. (2019). *Dissent on Aadhaar: Big data meets big brother*. Orient BlackSwan.

[51] O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown.

[52] Inzamam, Q., & Qadri, H. (2022, July 15). Telangana is inching closer to becoming a total surveillance state. *The Wire*.

[53] National Crime Records Bureau, Government of India. (n.d.). *Request for proposal to procure National Automated Facial Recognition System (AFRS)*. Retrieved January 6, 2026, from https://eprocure.gov.in/eprocure/app?component=%24DirectLink&page=FrontEndViewTender&service=direct&sp=S%2B6yRhk%2BPBLNDUmlDZkD8DQ%3D%3D

[54] Savyasachi, A. (2025, July 2). As AI took over policing in Delhi, who bore the brunt? *Pulitzer Center*.

[55] Bansal, V. (2022, August 21). The low threshold for face recognition in New Delhi. *Wired*.

[56] Press Information Bureau, Government of India. (2023, December 26). MeitY issues advisory to all intermediaries to comply with IT Rules, 2021 and existing laws: Deepfakes. Retrieved January 5, 2026, from https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1990542

[57] National e-Governance Division. (n.d.). Deepfakes in India: Legal landscape, judicial responses, and a practical playbook for enforcement. Retrieved January 6, 2026, from https://negd.gov.in/blog/deepfakes-in-india-legal-landscape-judicial-responses-and-a-practical-playbook-for-enforcement/

[58] Schick, N. (2020). *Deep fakes and the infocalypse: What you urgently need to know*. Octopus Publishing Group.

[59] *Case reported at* 2022 SCC OnLine Del 4110 (Delhi High Court, India).

[60] Gurumurthy, J. (2024). In the pursuance of a robust legal framework to address deepfake harms: An analysis of the Indian legal discourse. *Indian Journal of Law and Technology, 20*(1), Article 1.

[61] *Case reported at* CS(COMM) 652/2023 (Delhi High Court, India).

[62] Arora-Manohar, D., & Dey, S. (2025). The journalistic exemption under the Digital Personal Data Protection Act: A comparative study. *NUJS Law Review, 18*, 44.

[63] *Case reported at* W. P. (C) 235/2025 (Delhi High Court, India).

[64] Government of India, Ministry of Electronics and Information Technology. (n.d.). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*. Retrieved January 3, 2026, from https://www.meity.gov.in/content/information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021

[65] PRS Legislative Research. (2021). *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*. Retrieved January 4, 2026, from https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021

[66] Russell, S. J., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.

[67] Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.

[68] Bhardwaj, S., & Nayak, N. (2020). Rising internet shutdowns in India: A legal analysis. *Indian Journal of Law and Technology, 16*, 122–158.

[69] Gurumurthy, J. (2024). In the pursuance of a robust legal framework to address deepfake harms: An analysis of the Indian legal discourse. *Indian Journal of Law and Technology, 20*(1), Article 1.

[70] National Crime Records Bureau, Government of India. (n.d.). *Request for proposal for National Automated Facial Recognition System (NAFRS)*. Retrieved January 5, 2026, from https://ncrb.gov.in/TENDERS/AFRS/RFP_NAFRS.pdf

[71] Press Information Bureau, Government of India. (2024, March 7). Cabinet approves ambitious IndiaAI mission to strengthen the AI innovation ecosystem. Retrieved January 4, 2026, from https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2012357

[72] Bapat, K. (2022, January 3). Telangana High Court issues notice in India's first legal challenge to the deployment of facial recognition technology. *Internet Freedom Foundation*. Retrieved January 3, 2026, from https://internetfreedom.in/telangana-high-court-issues-notice-in-indias-first-legal-challenge-to-the-deployment-of-facial-recognition-technology/

[73] Carlini, N., Tramèr, F., Wallace, E., Jagielski, M., Herbert-Voss, A., Lee, K., Roberts, A., Brown, T., Song, D., Erlingsson, Ú., Oprea, A., & Raffel, C. (2021). Extracting training data from large language models. In *Proceedings of the 30th USENIX Security Symposium (USENIX Security 21)* (pp. 2633–2650). USENIX Association. Retrieved January 2, 2026, from https://www.usenix.org/system/files/sec21-carlini-extracting.pdf

[74] Dorwart, H., Gallan, J., & Rezzouk-Hammachi, V. (2023, October 13). Decrypting India's new data protection law: Key insights and lessons learned. *Bird & Bird*. Retrieved January 1, 2026, from

https://www.twobirds.com/en/insights/2023/global/decrypting-indias-new-data-protection-law-key-insights-and-lessons-learned

[75] Fredrikson, M., Lantz, E., Jha, S., Lin, S., Page, D., & Ristenpart, T. (2015). Model inversion attacks that exploit confidence information and basic countermeasures. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 1322–1333). Association for Computing Machinery. https://doi.org/10.1145/2810103.2813677

[76] Press Information Bureau, Government of India. (2025, November 17). *DPDP Rules, 2025 notified: A citizen-centric framework for privacy protection and responsible data use*. Retrieved January 2, 2026, from https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20251117695301.pdf

[77] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCR 569 (India). Retrieved January 9, 2026, from https://cdnbbsr.s3waas.gov.in/s3ec0490f1f4972d133619a60c30f3559e/documents/aor_notice_circular/43.pdf

[78] Indian Computer Emergency Response Team (CERT-In). (n.d.). Directions by CERT-In under Section 70B, Information Technology Act 2000. Retrieved January 1, 2026, from https://www.cert-in.org.in/Directions70B.jsp

[79] Latham & Watkins LLP. (2023, December). *India's Digital Personal Data Protection Act 2023 vs. the GDPR: A comparison*. Retrieved January 8, 2026, from https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf

[80] Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

[81] Savyasachi, A. (2025, July 2). As AI took over policing in Delhi, who bore the brunt? *Pulitzer Center*.

[82] Inzamam, Q., & Qadri, H. (2022, July 15). Telangana is inching closer to becoming a total surveillance state. *The Wire*.

[83] Government of India, Ministry of Electronics and Information Technology. (2021). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*. Retrieved January 10, 2026, from https://mib.gov.in/sites/default/files/2024-02/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf

[84] Bansal, V. (2022, August 21). The low threshold for face recognition in New Delhi. *Wired*.

[85] *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295 (India). Retrieved January 9, 2026, from https://indiankanoon.org/doc/619152/

[86] *Govind v. State of Madhya Pradesh*, (1975) 2 SCC 148 (India). Retrieved January 8, 2026, from https://indiankanoon.org/doc/436241/

[87] O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown.

[88] *Malak Singh v. State of Punjab & Haryana*, (1981). Retrieved January 7, 2026, from https://indiankanoon.org/doc/501107/

[89] *Selvi v. State of Karnataka*, (2010). Retrieved January 5, 2026, from https://indiankanoon.org/doc/127517806/

[90] *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997). Retrieved January 6, 2026, from https://indiankanoon.org/doc/91938676/

[91] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017). Retrieved January 4, 2026, from https://indiankanoon.org/doc/82461587/

[92] Fredrikson, M., Lantz, E., Jha, S., Lin, S., Page, D., & Ristenpart, T. (2015). Model inversion attacks that exploit confidence information and basic countermeasures. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 1322–1333). Association for Computing Machinery. https://doi.org/10.1145/2810103.2813677

[93] Shokri, R., Stronati, M., Song, C., & Shmatikov, V. (2017). Membership inference attacks against machine learning models. In *2017 IEEE Symposium on Security and Privacy (SP)* (pp. 3–18). IEEE.