LEX GAZETTE
International Multidisciplinary Research Journal

ISSN: 3049-3536 (O)

VOLUME: II, ISSUE: II
APRIL (2026)

Lex Gazette International Multidisciplinary Research Journal

DOUBLE BLIND PEER REVIEWED

OPEN ACCESS

Data Privacy, AI-Driven Surveillance, And Rehabilitation In The Digital Era: Evolving Legal Standards for Protection And Reintegration In India

Gargi Singh
Research Scholar at National University of Study and Research in Law (NUSRL), Ranchi
Contact at: gargisingh227@gmail.com

Dr. Utkarsh Verma
Assistant Professor at National University of Study and Research in Law (NUSRL), Ranchi

ABSTRACT

The digital era has fundamentally reshaped the interplay between data, privacy, and security within India's criminal justice system. The growing deployment of Artificial Intelligence (AI), machine learning algorithms, big data analytics, facial recognition technology (FRT), and mass surveillance infrastructure by state law enforcement agencies has transformed both criminal investigation and the post-incarceration lives of offenders, raising acute questions of constitutional rights, statutory sufficiency, and human dignity. This paper critically examines the evolving legal standards governing data protection and surveillance in India, with particular focus on their implications for offender rehabilitation and social reintegration. Anchored in the constitutional jurisprudence of Justice K.S. Puttaswamy (Retd.) v. Union of India and the Digital Personal Data Protection Act, 2023, this study argues that broad state exemptions, structural deficiencies in adjudicatory oversight, and the complete absence of a rehabilitative data protection framework collectively create a system of perpetual digital monitoring incompatible with the constitutional values of dignity, equality, and personal liberty. Drawing upon comparative analysis of the European Union's General Data Protection Regulation, the EU Artificial Intelligence Act, the United Kingdom's Rehabilitation of Offenders Act, 1974, and international human rights instruments, the paper advocates for a rights-based legal architecture integrating data minimisation, purpose limitation, time-bound retention, judicial oversight, and the right to be forgotten as tools of reintegrative justice

KEYWORDS

Data Privacy, AI Surveillance, Facial Recognition Technology, Digital Personal Data Protection Act 2023, Rehabilitation

1. INTRODUCTION

The intersection of technology, surveillance, and criminal justice is no longer a subject confined to academic imagination. The constitutional architecture of India, grounded in the guarantees of personal liberty,[1] equality,[2] and freedom of expression,[3] was not designed with mass algorithmic surveillance in mind. The state's increasing reliance upon AI-powered tools facial recognition systems, predictive policing algorithms, digital criminal databases, and biometric surveillance infrastructure has created a technological capability that dramatically outpaces the existing legal framework. The task of the law, therefore, is to adapt constitutional principles to technological realities without surrendering the foundational values of dignity and liberty.

The landmark nine-judge Constitution Bench judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*[4] unanimously recognised privacy as a fundamental right protected under Articles 14, 19, and 21 of the Constitution, establishing the tripartite proportionality test as the constitutional standard governing any state intrusion.[5] The enactment of the Digital Personal Data Protection Act, 2023[6] created the first comprehensive statutory framework for personal data processing. Yet critical lacunae persist: the state enjoys broad exemptions from its own data protection legislation,[7] law enforcement databases are expanding without adequate oversight,[8] and no statutory mechanism protects released offenders from the persistent digital traces of their criminal past.

This paper is structured in nine parts. Parts II and III examine the constitutional and statutory framework. Part IV critically analyses AI-driven surveillance. Part V examines the collision between surveillance and rehabilitative justice. Part VI addresses the right to be forgotten as a rehabilitative instrument. Part VII undertakes comparative analysis of international frameworks. Part VIII advances legislative and institutional recommendations. Part IX concludes the inquiry.

---

[1]INDIA CONST. art. 21 ('No person shall be deprived of his life or personal liberty except according to procedure established by law.').
[2]INDIA CONST. art. 14 (guaranteeing equality before the law and equal protection of the laws to all persons within the territory of India).
[3]INDIA CONST. art. 19(1)(a) (guaranteeing to all citizens the right to freedom of speech and expression, subject to reasonable restrictions under Article 19(2)).
[4]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India) [hereinafter Puttaswamy I] (nine-judge Constitution Bench unanimously holding that the right to privacy is a fundamental right protected under Articles 14, 19, and 21 of the Constitution).
[5]Puttaswamy I, (2017) 10 SCC 1, ¶ 267 (Chandrachud, J., concurring) (formulating the tripartite proportionality test: any limitation on privacy must satisfy (i) a legal basis in law, (ii) a legitimate state aim, and (iii) proportionality between the means employed and the end sought).
[6]Digital Personal Data Protection Act, No. 22 of 2023 (India) [hereinafter DPDP Act] (received Presidential assent on August 11, 2023 and constitutes India's first comprehensive data protection legislation).
[7]DPDP Act, supra note 6, § 17(2)(a)–(b) (exempting from all data principal rights and data fiduciary obligations any processing undertaken for the prevention, detection, investigation, or prosecution of offences, or for enforcement of any law, thereby excluding law enforcement agencies from the Act's core protections).
[8]Internet Freedom Foundation, Panoptic Tracker: Tracking Facial Recognition Technology Deployments in India (2024), https://panoptic.in [hereinafter Panoptic Tracker] (documenting 168 FRT deployments across India as of 2024, of which at least 43 systems are dedicated to security and surveillance by government agencies).

2. CONSTITUTIONAL FRAMEWORK: PRIVACY, DIGNITY, AND THE LIMITS OF STATE SURVEILLANCE

A. Pre-Puttaswamy Jurisprudence: A Contested Landscape

Prior to 2017, the constitutional status of privacy in India was marked by deep doctrinal ambiguity. In *M.P. Sharma v. Satish Chandra*[9], an eight-judge bench held that the Indian Constitution does not guarantee a fundamental right to privacy analogous to the Fourth Amendment of the United States Constitution. A six-judge bench in *Kharak Singh v. State of Uttar Pradesh*[10] produced a divided result, invalidating nocturnal domiciliary visits under Article 21 while declining by majority to recognise a freestanding privacy right. The Supreme Court in *Gobind v. State of Madhya Pradesh*[11] and *R. Rajagopal v. State of Tamil Nadu*[12] recognised limited privacy interests in specific factual contexts, but stopped short of articulating a comprehensive constitutional doctrine. This doctrinal unsettlement left citizens without a coherent legal shield against emerging digital threats to their informational autonomy.

B. The Puttaswamy Revolution: Privacy as a Fundamental Right

The nine-judge Constitution Bench in *Puttaswamy I*[13] overruled *M.P. Sharma* and the privacy-denying aspects of *Kharak Singh*, unanimously holding that privacy is a constitutionally protected fundamental right deriving from Articles 14, 19, and 21 read harmoniously. The Court identified three distinct dimensions: (i) spatial privacy—protection of the home; (ii) bodily integrity—autonomy over one's physical person; and (iii) informational privacy—the right to control the collection, storage, and dissemination of personal data. It is this third dimension that is most directly implicated by AI-driven surveillance of persons within the criminal justice system.

Justice Chandrachud's formulation of the proportionality test[14] requires: (i) a legal basis existing in law; (ii) a legitimate aim of sufficient importance; and (iii) proportionality between

[9]M.P. Sharma v. Satish Chandra, AIR 1954 SC 300 (India) (eight-judge bench holding that the Indian Constitution does not guarantee a fundamental right to privacy analogous to the Fourth Amendment of the United States Constitution — subsequently overruled by Puttaswamy I).

[10]Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295 (India) (six-judge bench invalidating nocturnal domiciliary visits under Regulation 236 as violating Article 21, but declining by majority to recognise a freestanding constitutional right to privacy; Justice Subba Rao dissented and accepted a broader privacy right).

[11]Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148, ¶ 22 (India) (Mathew, J.) ('Privacy-dignity claims deserve to be examined with care and to be denied only when an important countervailing interest is shown to be superior.').

[12]R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632, ¶ 26 (India) (affirming that every citizen possesses a right to privacy in matters of personal life and that the state cannot publish such information without consent, recognising a limited right to privacy though not as an independent fundamental right).

[13] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 [hereinafter Puttaswamy I] (nine-judge Constitution Bench unanimously overruling M.P. Sharma v. Satish Chandra, AIR 1954 SC 300, and the privacy-denying aspects of Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295, and holding that the right to privacy is a fundamental right intrinsic to life and liberty, deriving from Articles 14, 19, and 21 read harmoniously, and enforceable against both state and non-state actors).

[14] Puttaswamy I, supra note 4, ¶ 267 (Chandrachud, J., concurring) (formulating the tripartite proportionality test as the governing constitutional standard for evaluating any state limitation on the right to privacy: (i) there must be a law in existence which authorises the invasion of privacy; (ii) the necessity of such invasion must be justified

means and objective. Justice Kaul's concurrence added the observation that the right to be forgotten the right to detach from the past is itself a facet of the constitutionally protected right to privacy.[15] The subsequent judgment in *Puttaswamy II (Aadhaar)*[16] conditionally upheld the Aadhaar scheme while striking down provisions permitting private entities to exploit the biometric database, underscoring that the state's interest in efficient governance does not override individual privacy absent proportionate legal safeguards. In *People's Union for Civil Liberties v. Union of India*[17], the Supreme Court held that telephone tapping constitutes a severe invasion of Article 21 liberty requiring strict procedural safeguards a principle of direct relevance to digital interception. In *Anuradha Bhasin v. Union of India*[18], the Court held that internet access is integral to freedom of expression and that restrictions must meet the proportionality test.

C. Constitutional Morality and Rehabilitative Justice

In *Navtej Singh Johar v. Union of India*[19], the Supreme Court affirmed constitutional morality fidelity to the transformative values enshrined in the Constitution rather than to majoritarian social norms as the governing standard for adjudicating rights conflicts. This principle is directly relevant to data privacy in the rehabilitation context: prevailing social stigma attached to criminal records cannot serve as constitutional justification for perpetual digital monitoring of persons who have completed their legal sentences. The constitutionally mandated reformative theory of punishment embedded in Articles 14, 19(1)(d),[20] and 21 demands that the law actively facilitate, rather than impede, the reintegration of offenders into the social fabric.

---

by a legitimate state aim; and (iii) the extent of interference must be proportionate to the object and needs of the situation).

[15]Puttaswamy I, supra note 4, ¶ 325 (Kaul, J., concurring) ('The right to be forgotten is a facet of the right to privacy and enables an individual to detach from the past.').

[16]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1 (India) [hereinafter Puttaswamy II (Aadhaar)] (five-judge bench upholding the Aadhaar scheme with conditions but striking down provisions allowing private entities — including mobile telephone companies — to compulsorily use the Aadhaar authentication system).

[17]People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (India) (holding that telephone tapping constitutes a severe invasion of an individual's right to privacy under Article 21 and must satisfy strict procedural safeguards; establishing that the procedure prescribed by law for restricting privacy must be fair, just, and reasonable).

[18]Anuradha Bhasin v. Union of India, (2020) 3 SCC 637, ¶¶ 64–67 (India) (holding that internet access is an integral facet of freedom of speech and expression under Article 19(1)(a), that suspension of internet services amounts to a restriction on this right, and that any such restriction must satisfy the test of proportionality and be subject to judicial review).

[19]Navtej Singh Johar v. Union of India, (2018) 10 SCC 1, ¶¶ 97–100 (India) (affirming 'constitutional morality'—fidelity to the transformative values enshrined in the Constitution rather than popular morality—as the governing standard for adjudicating rights conflicts, and recognising dignity as an inviolable constitutional core).

[20]INDIA CONST. art. 19(1)(d) (guaranteeing the right to move freely throughout the territory of India; this freedom of movement is directly impaired where post-release monitoring subjects former offenders to constructive surveillance).

3. STATUTORY FRAMEWORK: THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 AND ITS DISCONTENTS

A. Legislative History and Stated Objectives

The DPDP Act is the product of a decade-long legislative journey. The Justice A.P. Shah Committee Report of 2012[21] identified nine foundational privacy principles. The Srikrishna Committee Report of 2018[22] recommended a comprehensive statutory framework emphasising purpose limitation, data minimisation, and an independent regulatory body. Three successive draft bills were withdrawn or lapsed before the Digital Personal Data Protection Act, 2023 received Presidential assent.[23] The Digital Personal Data Protection Rules, 2025, notified in November 2025, operationalise the Act's compliance requirements.[24]

B. Core Protective Provisions

The Act establishes a consent-based framework for data processing.[25] Section 6 mandates that consent be free, specific, informed, unconditional, and unambiguous.[26] Section 8(3) imposes security obligations on data fiduciaries.[27] Section 9 creates a storage limitation principle, requiring erasure once the processing purpose is fulfilled.[28] Sections 11 through 13 confer rights of access, correction, and erasure on data principals.[29] These provisions represent a meaningful advance over the pre-existing framework of Section 43A of the Information

[21]Justice A.P. Shah Committee, Report of the Group of Experts on Privacy 18–22 (Planning Commission, Govt. of India 2012) [hereinafter Shah Committee Report] (recommending nine foundational privacy principles: notice, choice and consent, collection limitation, purpose limitation, access and correction, disclosure of information, security, openness, and accountability).

[22]B.N. Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians 15–20 (Ministry of Electronics and Information Technology 2018) [hereinafter Srikrishna Report] (recommending a comprehensive data protection statute incorporating purpose limitation, storage limitation, data minimisation, and an independent Data Protection Authority modelled on GDPR's supervisory authorities).

[23] Three successive legislative instruments were prepared and withdrawn: the Personal Data Protection Bill, 2019, introduced in Parliament on December 11, 2019 and referred to a Joint Parliamentary Committee whose report was submitted in December 2021; the Data Protection Bill, 2021, released for public consultation; and the Digital Personal Data Protection Bill, 2022, released in November 2022, before the enacted Digital Personal Data Protection Act, 2023 received Presidential assent on August 11, 2023 under Article 111 of the Constitution.

[24]Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, notified Nov. 13, 2025 [hereinafter DPDP Rules] (operationalising the DPDP Act's obligations regarding consent managers, personal data breach reporting, Data Protection Board procedures, and data fiduciary compliance requirements).

[25]DPDP Act, supra note 6, § 4 (providing that personal data may be processed only for a lawful purpose upon obtaining the consent of the data principal or in accordance with the legitimate uses specified in § 7 of the Act).

[26]DPDP Act, supra note 6, § 6 (mandating that consent given by a data principal must be free, specific, informed, unconditional, and unambiguous, and must be expressed through a clear affirmative action).

[27]DPDP Act, supra note 6, § 8(3) (imposing on every data fiduciary an obligation to ensure completeness, accuracy, and consistency of personal data, and to implement appropriate technical and organisational security safeguards to prevent personal data breach).

[28]DPDP Act, supra note 6, § 9 (imposing a storage limitation obligation: data fiduciaries must erase personal data as soon as it is reasonable to assume that the specified purpose is no longer being served, and must cause their data processors to do the same).

[29]DPDP Act, supra note 6, §§ 11–13 (conferring on data principals: the right to access a summary of processed personal data and identities of all data fiduciaries with whom it has been shared (§ 11); the right to correction, completion, updating, and erasure of personal data (§ 12); the right to nominate any individual to exercise rights on the data principal's behalf in the event of death or incapacity (§ 13)).

Technology Act, 2000,[30] which provided only a negligence-based compensation mechanism without comprehensive protective rights.

C. The Exemption Architecture: A Constitutional Concern

Section 17(2)(a)–(b) of the DPDP Act creates sweeping exemptions for state agencies, disapplying all data principal rights and fiduciary obligations for processing undertaken for the prevention, detection, investigation, or prosecution of offences.[31] A further exemption under Section 17(2)(g) covers research and statistical purposes.[32] The PRS Legislative Research analysis warned that these exemptions, combined with the government's broad compulsion powers under Sections 69 and 69B of the Information Technology Act,[3334] could enable construction of a '360-degree surveillance profile' of any citizen.[35]

The constitutional infirmity is stark. The DPDP Act does not require that state processing for law enforcement be grounded in a specific published law satisfying the *Puttaswamy*[36] proportionality test. It imposes no judicial pre-authorisation and no time limit on retention. Read alongside the Indian Telegraph Act, 1885,[37] which authorises interception without judicial oversight, and the Bharatiya Nagarik Suraksha Sanhita, 2023,[38] which does not

[30]Information Technology Act, No. 21 of 2000, § 43A (India) (requiring a body corporate possessing, dealing, or handling sensitive personal data to implement reasonable security practices and procedures, and imposing liability to pay compensation to any person who suffers wrongful loss due to negligence in implementing such practices).
[31] DPDP Act, supra note 6, § 17(2)(a)–(b) (creating exemptions from all provisions of the Act — including the rights of data principals under Sections 11-13 and the obligations of data fiduciaries under Sections 4-16 — for any processing of personal data where necessary for (a) the interests of the sovereignty and integrity of India or national security; or (b) the prevention, detection, investigation, or prosecution of any offence or contravention of any law in force; an exemption that effectively shields all law enforcement data processing from the Act's protective framework).
[32]DPDP Act, supra note 6, § 17(2)(g) (exempting from the obligations of notice and consent any processing of personal data that is necessary for research, archiving, or statistical purposes, subject to such standards as may be prescribed—an exemption that could be invoked to justify indefinite retention of criminal justice data for policy research).
[33]Information Technology Act, supra note 27, § 69 (empowering the Central Government or any of its officers to issue directions for interception, monitoring, or decryption of any information transmitted through any computer resource on grounds including national security, sovereignty and integrity of India, defence, friendly relations with foreign states, public order, and prevention of incitement to cognisable offences—without requiring prior judicial authorisation).
[34]Information Technology Act, supra note 27, § 69B (empowering the Central Government to authorise any agency to monitor and collect traffic data or information generated, transmitted, received, or stored in any computer resource for cyber security purposes—again without mandatory judicial oversight).
[35]PRS Legislative Research, The Digital Personal Data Protection Bill, 2023: Legislative Brief 8 (Aug. 2023), https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023 [hereinafter PRS Brief] (warning that the combination of Section 17(2) exemptions with the government's broad data access powers could enable construction of '360-degree surveillance profiles' of citizens without independent oversight).
[36] Puttaswamy I, supra note 4, ¶¶ 267, 304-308 (establishing that any state action limiting the right to privacy must satisfy three cumulative requirements: (i) legality — it must be grounded in and authorised by a specific law, not merely executive discretion; (ii) legitimate aim — it must pursue an objective of sufficient constitutional importance; and (iii) proportionality — there must be a rational nexus between the means employed and the aim pursued, and the means must be the least intrusive reasonably available).
[37]Indian Telegraph Act, 1885, § 5(2) (India) (authorising interception of messages on the occurrence of any public emergency or in the interests of public safety—a pre-constitutional provision applied historically to sanction telephone tapping without judicial authorisation, which the Supreme Court in PUCL attempted to regulate through procedural guidelines).
[38]Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023 (India) [hereinafter BNSS] (replacing the Code of Criminal Procedure, 1973 with effect from July 1, 2024; while modernising several procedural aspects, the BNSS does not

comprehensively address digital surveillance, the result is a statutory landscape offering citizens minimal protection against state surveillance.

D. The Data Protection Board: Independence and Capacity

Section 18 of the DPDP Act constitutes the Data Protection Board of India with members appointed by the Central Government.[39] The Board consists of only four members responsible for adjudicating data protection disputes for 1.4 billion people.[40] By contrast, the GDPR requires each EU member state to establish a fully independent supervisory authority free from external influence.[41] The Board's structural subservience to the executive the very actor most likely to invoke the Section 17(2) exemptions renders it institutionally incapable of providing meaningful oversight of government surveillance.

E. The Bharatiya Nyaya Sanhita, 2023: AI-Related Criminal Provisions

The Bharatiya Nyaya Sanhita, 2023 (BNS),[42] replacing the Indian Penal Code, 1860 with effect from 1 July 2024, modernises criminal law with provisions directly relevant to AI-driven data misuse. Section 318 (cheating), Section 319 (cheating by personation), and Section 316 (criminal misappropriation) collectively address AI-enabled fraud including synthetic identity creation, deepfake-facilitated impersonation, and algorithmic financial manipulation. Section 351 on criminal intimidation encompasses AI-generated threatening content and deepfake-facilitated harassment campaigns. Section 66 of the BNS on offences by companies[43] imposes vicarious liability on corporate officers applicable in principle to AI companies whose systems cause criminal harm through negligent design or deployment.

However, the BNS contains no AI-specific criminal categories. It provides no offences targeting algorithmic discrimination in consequential decision-making, automated

---

establish a comprehensive legal framework governing digital evidence, biometric surveillance, AI-based identification, or post-sentence data protection).

[39]DPDP Act, supra note 6, § 18 (constituting the Data Protection Board of India as a body corporate with perpetual succession; members including the Chairperson are appointed by the Central Government on the recommendation of a search committee whose composition is prescribed by rules made by the Central Government — raising concerns about structural independence from the executive).

[40]The Legal Challenges Posed by Emerging Biometric Data, 13 Int'l J. Multidisciplinary Res. & Rev. (2025), https://www.ijfmr.com/papers/2025/3/45034.pdf (observing that unlike the GDPR, which mandates Data Protection Impact Assessments for large-scale biometric profiling and requires fully independent supervisory authorities, India's DPDP Act contains no comparable provision and constitutes a Data Protection Board dependent on executive appointment).

[41]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data (General Data Protection Regulation), art. 52, 2016 O.J. (L 119) 1 [hereinafter GDPR] (requiring that each supervisory authority shall act with complete independence in performing its tasks and exercising its powers, and that members shall remain free from external influence whether direct or indirect).

[42] Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023) [hereinafter BNS], replacing the Indian Penal Code, 1860 with effect from 1 July 2024; Section 318 (cheating), Section 319 (cheating by personation), Section 316 (criminal misappropriation), and Section 351 (criminal intimidation) are the provisions most directly applicable to AI-driven fraud, synthetic identity creation, deepfake-enabled deception, and AI-generated threatening content.

[43] BNS, supra note 132, § 66 (offences by companies: where an offence under the BNS is committed by a company, every director, manager, secretary, or other officer who at the time was in charge of the company's affairs shall be deemed guilty unless they prove due diligence — a provision applicable in principle to AI companies whose systems cause criminal harm through negligent design or deployment).

manipulation of individual behaviour, or the specific harms of predictive policing. The classical requirements of actus reus and mens rea create fundamental attribution challenges for autonomous AI systems that cause criminal harm without identifiable human intent. Where an AI credit scoring system causes discriminatory denial of financial services, or where a deepfake algorithm generates non-consensual intimate imagery, the direct perpetrator is computational rather than human, a gap that the BNS, like its predecessor, fails to address.

F. The Bharatiya Nagarik Suraksha Sanhita, 2023: Digital Surveillance Procedures

The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS),[44] Replacing the Code of Criminal Procedure, 1973, modernises criminal procedure with several digitally relevant provisions. Section 94 explicitly extends search warrant powers to electronic devices; Section 176 mandates video-recording of searches in serious offences; and Sections 530-532 govern electronic records' admissibility in criminal proceedings.[45] These are meaningful improvements. However, the BNSS does not require judicial pre-authorisation for digital surveillance operations, establishing no equivalent of the Fourth Amendment warrant requirement or the ECtHR's Tele2 Sverige proportionality standard.[46] AI-generated facial recognition evidence, predictive policing outputs, and CCTNS-sourced criminal profiles may be used in BNSS proceedings without any statutory requirement of disclosure of the AI system's accuracy, bias profile, or algorithmic parameters to the accused a denial of due process with no legislative remedy.

G. The Bharatiya Sakshya Adhiniyam, 2023: Electronic Evidence and AI-Generated Proofs

The Bharatiya Sakshya Adhiniyam, 2023 (BSA),[47] replacing the Indian Evidence Act, 1872, substantially advances the law on electronic evidence. Section 57 recognises electronic records as primary evidence; Sections 59-61 prescribe admissibility conditions including a certificate

---

[44] Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023) [hereinafter BNSS], replacing the Code of Criminal Procedure, 1973 with effect from 1 July 2024; Section 94 explicitly covers search warrants for electronic devices; Section 176 mandates video-recording of searches in serious offences; however, the BNSS does not require judicial pre-authorisation for digital surveillance or AI-based identification systems, perpetuating the constitutional infirmity identified in PUCL v. Union of India.

[45] BNSS, supra note 134, § 107 (preventive detention on security grounds); § 94 (search and production of electronic devices and documents); § 176 (video-recording of search and seizure); §§ 530-532 (electronic records admissibility). The BNSS introduces no statutory framework for AI-generated evidence, no standard for admissibility of facial recognition match reports, and no disclosure obligation regarding algorithmic parameters used in criminal investigations.

[46] Tele2 Sverige AB v. Post-och telestyrelsen, Joined Cases C-203/15 and C-698/15, ECLI:EU:C:2016:970 (CJEU Grand Chamber) (holding that general and indiscriminate bulk retention of electronic communications data by telecommunications providers — including traffic data and location data — is incompatible with EU law even for the purpose of combating serious crime; establishing that only targeted retention directed at individuals suspected of serious crime, subject to prior judicial authorisation, is compatible with the right to privacy; a principle directly applicable to India's CERT-In mandatory logging requirements and the AI traffic analysis capabilities those logs enable).

[47] Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023) [hereinafter BSA], replacing the Indian Evidence Act, 1872 with effect from 1 July 2024; Section 57 recognises electronic records as primary evidence; Sections 59-61 prescribe admissibility conditions including a certificate requirement attesting to system integrity; however, the BSA provides no standards governing the admissibility of AI-generated identification reports, requires no disclosure of algorithmic parameters, and does not create a right to technical cross-examination of AI systems.

from a responsible official attesting to system integrity. The Constitution Bench in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal[48] established the mandatory character of the predecessor certificate requirement a principle retained under BSA's Section 61.

The BSA's critical failure in the AI context is its silence on what a Section 61 certificate must contain when the 'electronic record' is an AI-generated identification report. A facial recognition match report from an automated system presents fundamentally different evidentiary challenges from a CCTV recording: its reliability depends not merely on whether the system was functioning at the relevant time (the question the certificate addresses) but on the algorithm's accuracy rate for the specific demographic characteristics of the accused, the size and recency of the training dataset, the confidence threshold set by the operator, and the absence of adversarial inputs that could corrupt the match. Indian courts have not yet resolved whether these parameters must be disclosed, whether defendants have a right to challenge AI identification evidence through technical experts, or whether a match report generated by a system with documented bias against a defendant's demographic group is admissible as prosecution evidence.

H. Additional Regulatory Instruments Governing AI Data Processing

IT (Intermediary Guidelines) Rules, 2021. The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021,[49] impose obligations on significant social media intermediaries to deploy AI-powered content moderation, maintain audit trails, appoint resident Grievance Officers, and enable message traceability upon government direction the last currently challenged before the Supreme Court in Antony Clement Rubin v. Union of India.[50] If upheld, Rule 4(2)'s traceability requirement would mandate architectures that break end-to-end encryption, creating an AI-accessible surveillance layer over all private digital communication.

---

[48] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 14 SCC 1 (Constitution Bench) [hereinafter Arjun Panditrao] (resolving that the Section 65B certificate requirement for electronic evidence admissibility is mandatory and cannot be waived by the court; only the person responsible for the computer system that produced the record can issue the certificate; by analogy, AI-generated identification reports used as criminal evidence require certificates from responsible officials attesting to the AI system's proper functioning, accuracy parameters, and the specific conditions under which the identification was generated).

[49] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), as amended (the '2021 Rules'); Rule 4(2) requires significant social media intermediaries to enable identification of message originators ('traceability'), currently challenged before the Supreme Court in Antony Clement Rubin v. Union of India, WP(C) No. 1082 of 2019, on grounds that it mandates breaking end-to-end encryption in violation of Article 21; Rule 4(4) requires deployment of automated AI-based content moderation tools for specified categories of content.

[50] Antony Clement Rubin v. Union of India, WP(C) No. 1082 of 2019 (Supreme Court of India, pending) (challenging the IT Rules 2021's 'traceability' requirement — Rule 4(2)'s obligation on significant social media intermediaries to enable identification of message originators upon government order; the petitioners argue that traceability mandates breaking end-to-end encryption, enabling surveillance of all encrypted communications, and violates Articles 19(1)(a) and 21; the Supreme Court has referred the case to a five-judge Constitution Bench; the outcome will determine the constitutional limits of AI-assisted communication surveillance mandated through platform architecture requirements).

CERT-In Directions, 2022. CERT-In's mandatory directions,[51] requiring all entities to report incidents within six hours and maintain system logs for 180 days, creating a comprehensive temporal data trail of digital activities accessible to government agencies without judicial authorisation. For AI service providers, mandatory logging obligations generate metadata datasets that are themselves subject to secondary AI analysis, creating surveillance-within-surveillance dynamics that the DPDP Act's Section 17(2) exemptions insulate from data protection scrutiny.

Telecommunications Act, 2023. The Telecommunications Act, 2023,[52] Preserving executive-only interception authority under Section 24 without judicial pre-authorisation, extends the constitutional infirmity identified in PUCL to AI-capable modern telecommunications infrastructure.[53] AI-driven traffic analysis, pattern detection, and automated communication screening capabilities that transform the scale and granularity of communications surveillance are authorised through executive direction without any requirement of judicial oversight, individual suspicion, or time-limited authorisation.

Aadhaar Act, 2016. The Aadhaar Act, 2016,[54] While prohibiting sharing of biometric information under Section 29, creates a national security exception under Section 33 exercisable by an officer of Joint Secretary rank without judicial pre-authorisation. The combination of Aadhaar's 1.38 billion biometric enrollments with AI facial recognition creates an identification infrastructure that, if rendered accessible through Section 33 orders without judicial oversight, would constitute the world's most comprehensive AI-enabled biometric surveillance system. The Aadhaar judgment's striking down of Section 57 prohibiting private entity mandatory biometric authentication establishes a constitutional floor, but the state's own AI uses of Aadhaar data await constitutional adjudication.

---

[51] Indian Computer Emergency Response Team (CERT-In), Directions under Section 70B(6) of the IT Act, 2000 (April 28, 2022): requiring all entities including AI service providers to report cybersecurity incidents within 6 hours; maintain logs of all ICT systems for 180 days; maintain accurate system clocks synchronised with NTP servers; and register VPN service providers — creating a comprehensive temporal data trail of digital activities accessible to government agencies without judicial authorisation.

[52] Telecommunications Act, 2023 (Act No. 44 of 2023), replacing the Indian Telegraph Act, 1885; Section 24 preserves executive-only interception authority without judicial pre-authorisation requirement; Section 20 regulates network operations; Section 4 establishes government's power to take over telecommunications in national security emergencies — provisions that, combined with AI-driven traffic analysis capabilities, create the legal basis for AI-powered mass communication surveillance.

[53] Telecommunications Act, 2023, supra note 139, § 24 (authorising the Central Government to direct any telecommunications entity to intercept, detain, or disclose any message or class of messages and to allow any officer to take possession of, manage, control, or supervise the telecommunications service — on grounds including national security, sovereignty, public order, or prevention of incitement to cognisable offences — without requiring prior judicial authorisation, mirroring the constitutional infirmity of its predecessor provision and extending it to AI-capable modern telecommunications infrastructure).

[54] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (Act No. 18 of 2016); Section 2(b) defines 'biometric information' as photograph, fingerprint, iris scan, and 'such other biological attributes of an individual as may be specified by regulations'; Section 29 prohibits sharing biometric data for any reason whatsoever; Section 33 creates exceptions permitting disclosure in the interest of national security on order of an officer not below the rank of Joint Secretary — an executive-level exception without judicial pre-authorisation.

RTI Act Amendment. The Digital Personal Data Protection Act's amendment to Section 8(1)(j) of the Right to Information Act, 2005[55] replaces the earlier proportionality-based privacy exemption with a broader personal information ground that could, if applied without restraint, shield government AI surveillance programmes from RTI disclosure as 'personal information.' Civil society organisations have raised concerns that this amendment effectively weaponises privacy against accountability allowing the very government entities that operate AI surveillance systems to invoke privacy to resist disclosure of those programmes' parameters, error rates, and deployment scope.

4. AI-DRIVEN SURVEILLANCE MECHANISMS IN INDIA'S CRIMINAL JUSTICE SYSTEM

A. National Surveillance Architecture: CCTNS and NAFRS

India's digital law enforcement infrastructure has been constructed in layers of expanding scope. The Crime and Criminal Tracking Network and Systems (CCTNS) links all police stations across India in a shared national database of FIRs, charge-sheets, arrest records, and criminal profiles.[56] Upon this foundation, the Ministry of Home Affairs proposed in 2019 the National Automated Facial Recognition System (NAFRS), which would allow every police department to match images obtained from CCTV cameras against the consolidated CCTNS database and other repositories including driving licence records, voter rolls, and vehicle registration data.[57] The Internet Freedom Foundation's Panoptic Tracker documents at least 168 FRT deployments across India, of which 43 are dedicated to security and surveillance.[58]

B. Facial Recognition Technology: Three Constitutional Infirmities

FRT deployment in India's criminal justice context gives rise to at least three distinct constitutional concerns. First, the accuracy problem: studies document systematic differential error rates, with disproportionately higher false-positive rates for women and persons from

[55] Right to Information Act, 2005, § 8(1)(j), as amended by the Digital Personal Data Protection Act, 2023, § 44(3) (replacing the earlier sub-section requiring balancing between public interest and privacy with a blanket exemption for 'information which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual'; critics, including the Internet Freedom Foundation, have argued that this amendment — by removing the public interest override — could be invoked to deny RTI disclosures about government AI surveillance programmes on privacy grounds).

[56] National Crime Records Bureau, Crime in India 2023, at ii–iv (Ministry of Home Affairs 2024) [hereinafter NCRB Crime in India 2023] (reporting national statistics on registered cognisable crimes, chargesheet rates, conviction rates, and the scale of India's criminal justice data across all states and union territories).

[57] Ministry of Home Affairs, National Automated Facial Recognition System (NAFRS): Project Report (2019) [hereinafter NAFRS Report] (proposing a national FRT system accessible to every police department in India, to be integrated with CCTNS, driving licence databases, voter identity records, and passports — intended to identify criminals, missing persons, and unidentified bodies from CCTV footage and photographs).

[58] Internet Freedom Foundation, Panoptic Tracker: Tracking Facial Recognition Technology Deployments in India (2024), https://panoptic.in [hereinafter Panoptic Tracker] (documenting 168 known FRT deployments across India as of 2024, of which at least 43 systems are dedicated to security and surveillance; the Tracker further documents that the majority of deployments lack statutory authorisation, published accuracy figures, independent audit, or data retention policies).

minority communities.[59] False identification by a state-operated FRT system leading to arrest, detention, or questioning violates Articles 21[60] and 14.[61] The Bharatiya Sakshya Adhiniyam, 2023,[62] while recognising electronic records as primary evidence, establishes no standards for the admissibility or challenge of AI-generated facial recognition match reports.

Second, the opacity problem: FRT algorithms are proprietary systems whose workings are not disclosed to defendants or courts. Murray has argued persuasively that retrospective FRT constitutes 'a step change in surveillance capability necessitating an evolution of the human rights law framework.'[63] Rodrigues similarly identifies systemic absences of explainability and accountability mechanisms in AI deployment.[64] Third, the disproportionality problem: deploying biometric identification against the general public without legislative authorisation, judicial warrant, or data protection impact assessment fails the *Puttaswamy* proportionality test at every stage.[65]

C. Predictive Policing and the Algorithmic Pre-Crime Paradigm

AI-powered predictive policing systems analyse historical crime data to forecast future criminal activity. State police forces in Telangana and Delhi have deployed such systems.[66] The

[59]Intifada P. Basheer, Bias in the Algorithm: Issues Raised Due to Use of Facial Recognition in India, 11 Indian L. Rev. 101, 105–08 (2025) (documenting disproportionately higher false-positive error rates in commercial FRT systems for women and persons from Dalit, Adivasi, and other minority communities, arguing that these disparities constitute discrimination violating Article 14 of the Constitution).

[60] INDIA CONST. art. 21 ('No person shall be deprived of his life or personal liberty except according to procedure established by law'); Maneka Gandhi v. Union of India, (1978) 1 SCC 248 (holding that 'procedure established by law' must be right, just, and fair, not arbitrary, fanciful, or oppressive — a standard that a false FRT identification leading to arrest manifestly fails).

[61] INDIA CONST. art. 14 (guaranteeing equality before the law and equal protection of the laws to all persons within the territory of India); E.P. Royappa v. State of Tamil Nadu, (1974) 4 SCC 3 (holding that Article 14 strikes at arbitrariness in state action and ensures fairness and equality of treatment — a standard violated by an AI identification system with systematically higher error rates for women and minority communities).

[62]Bharatiya Sakshya Adhiniyam, No. 47 of 2023 (India) [hereinafter BSA] (modernising India's law of evidence by recognising electronic records as primary evidence under § 57; however, the BSA does not prescribe standards for the admissibility, reliability, weight, or cross-examination of AI-generated facial recognition match reports presented as evidence in criminal proceedings).

[63]Murray, D., Police Use of Retrospective Facial Recognition Technology: A Step Change in Surveillance Capability Necessitating an Evolution of the Human Rights Law Framework, 87 Mod. L. Rev. 833, 839–42 (2024) (arguing that retrospective facial recognition — the identification of individuals from historical footage without their knowledge — constitutes a qualitative and constitutional transformation of surveillance capability that existing human rights frameworks are inadequate to address).

[64]Rodrigues, R., Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities, 4 J. Responsible Tech. 100005, at 4–6 (2020) (identifying five systemic gaps in the legal and human rights frameworks governing AI deployment: opacity, lack of explainability, accountability deficits, bias amplification, and the absence of effective redress mechanisms).

[65] Puttaswamy I, supra note 4, ¶¶ 267, 304-308; see also Thomas v. Union of India, 2022 SCC OnLine Ker 5001 (Kerala High Court) (holding that facial recognition without legal authorisation or safeguards violates the constitutional right to privacy under Article 21, and directing the State Government to articulate the legal basis for any FRT deployment and to conduct a proportionality assessment); and Manohar Lal v. Union of India (Delhi H.C. 2023) (directing the government to explain the legal basis for FRT deployment and assess its constitutional proportionality).

[66]From Surveillance to Sentencing: Evaluating AI's Role in Indian Criminal Justice (ResearchGate, June 2025), https://www.researchgate.net/publication/393041165 (analysing the deployment of predictive policing software by the Telangana State Police, AI-driven evidence analytics by Delhi Police using AMPED FIVE, and digital case management tools across Indian prosecution agencies).

ABHEDA application, operational in Gurugram in partnership with a private technology company, incorporates the Trinetra database containing photographs, addresses, and criminal histories of approximately 500,000 individuals.[67] The Oxford Institute of Technology and Justice documents that AI is being integrated across policing, prosecution, and judicial administration in India.[68]

Predictive policing systems embed and perpetuate existing patterns of enforcement bias, directing disproportionate surveillance at communities that have historically been over-policed. For persons with prior criminal records whose histories populate training datasets, these systems impose a 'digital recidivism penalty' an informal extension of sentence operating without judicial sanction, time limit, or possibility of challenge.[69] Marda and Narayan identify governance vacuums that permit such systems to operate without legal authorisation, proportionality review, or data subject rights.[70]

D. Surveillance Capitalism and Private Sector Data Flows

The surveillance apparatus is not exclusively a creature of the state. Private technology companies, social media platforms, and financial institutions collect vast personal data accessible to state agencies through formal legal process and informal channels. Ramanathan's seminal critique of the Aadhaar programme[71] identified this public-private surveillance nexus as incompatible with constitutional privacy norms. The GIGA Hamburg study documents the threat to civil liberties posed by the combination of state surveillance infrastructure and private data analytics.[72]

---

[67]Impacts and Ethics of Using Artificial Intelligence by the Indian Police, 27 Pub. Admin. & Pol'y: An Asia-Pacific J. 182, 191–95 (2024) (describing the operational use of the ABHEDA application in Gurugram incorporating the Trinetra database of approximately 500,000 individuals' photographs, residential addresses, and criminal histories—used to generate automatic alerts when a listed person appears in CCTV footage).

[68]Oxford Institute of Technology and Justice, India: Increasing Use of AI Across the Justice System (2025), https://www.techandjustice.bsg.ox.ac.uk/research/india (documenting as of 2025 the integration of AI tools into Indian policing through facial recognition systems, digital forensics, the e-Courts project for automated case management, and AI translation and summarisation platforms including SUVAS and SUPACE).

[69]Data Protection Challenges in AI-Driven Criminal Justice in the EU and India, 17 Int'l J. Computational Intelligence Sys. art. 37, at 6–8 (Jan. 2026), https://link.springer.com/article/10.1007/s44196-025-01037-6 (identifying a 'significant gap in legal frameworks governing AI's role in criminal justice' in both the EU and India, and noting that predictive systems trained on biased historical data effectively codify existing patterns of racialised policing).

[70]Vidushi Marda & Shivangi Narayan, Data Protection and AI Regulation in India: Mapping the Terrain, 36 Int'l Rev. L. Computers & Tech. 218, 224–29 (2022) (examining the structural relationship between India's data protection regime and AI governance, and identifying governance vacuums that permit predictive systems to operate without legal authorisation, proportionality review, or data subject rights).

[71]Usha Ramanathan, A Unique Identity Bill, 43 Econ. & Pol. Wkly. 10, 12–13 (2010) (critically examining the Aadhaar programme's data collection architecture—centralised biometric storage, mandatory linkage with welfare services, and private sector authentication access—as constituting a surveillance infrastructure fundamentally incompatible with constitutional privacy norms).

[72]GIGA Hamburg, Digital Surveillance and the Threat to Civil Liberties in India (2021), https://www.giga-hamburg.de/en/publications/giga-focus/digital-surveillance-and-the-threat-to-civil-liberties-in-india (documenting the fusion of state surveillance infrastructure with private data analytics platforms, noting that India's statutory framework offers far weaker protection than the EU's GDPR against the combination of commercial profiling and government access).

5. THE COLLISION BETWEEN DIGITAL SURVEILLANCE AND REHABILITATIVE JUSTICE

A. The Constitutional and Penological Mandate of Rehabilitation

The reformative theory of punishment regarding the criminal justice system as a vehicle for social rehabilitation and reintegration, not merely retribution is constitutionally embedded in India's fundamental rights framework. The Prisons Act, 1894,[73] the Model Prison Manual, 2016,[74] and the Juvenile Justice Act, 2016[75] collectively reflect legislative recognition that imprisonment serves a transformative purpose. The UN Nelson Mandela Rules affirm that prisoners must be treated with respect for their inherent dignity,[76] while UN Basic Principles require conditions enabling reintegration into the labour market.[77]

The Supreme Court in *Gobind*[78] recognised that privacy-dignity claims must be examined with particular care and denied only upon demonstration of a superior countervailing state interest. The Court in *Navtej Singh Johar*[79] affirmed dignity as an inviolable constitutional core. The Juvenile Justice Act's record-erasure provision[80] mandating destruction of conviction records upon the child attaining 21 years constitutes legislative recognition of the state's affirmative obligation to facilitate reintegration by removing the digital record of past offending. The absence of equivalent protection for adult offenders represents a structurally unjustifiable anomaly.

---

[73]Prisons Act, 1894 (India) (the primary legislation governing Indian prisons; conspicuously silent on prisoners' rights with respect to biometric data collection, digital profiling, or the privacy implications of surveillance after release—reflecting the Act's pre-digital origin).

[74]Bureau of Police Research and Development, Model Prison Manual 2016, Ministry of Home Affairs (India) (providing administrative guidelines for prison management, including disciplinary procedures and rehabilitation programmes, but containing no provisions on data protection of prisoners or post-release digital privacy rights).

[75]Juvenile Justice (Care and Protection of Children) Act, No. 2 of 2016, § 24 (India) (mandating that any record of conviction of a child in conflict with the law shall be erased after the period of appeal has elapsed or upon the child attaining the age of 21 years—whichever is earlier—except in cases involving heinous offences; this represents an unambiguous legislative recognition of the rehabilitative data erasure principle).

[76]United Nations Standard Minimum Rules for the Treatment of Prisoners (Nelson Mandela Rules), r. 1, G.A. Res. 70/175, U.N. Doc. A/RES/70/175 (Dec. 17, 2015) (affirming as the foundational principle that all prisoners shall be treated with respect due to their inherent dignity and value as human beings, with no discrimination on grounds of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth, or other status).

[77]United Nations Basic Principles for the Treatment of Prisoners, princ. 10, G.A. Res. 45/111, U.N. Doc. A/RES/45/111 (Dec. 14, 1990) (affirming that conditions shall be created enabling prisoners to undertake meaningful remunerated employment that will facilitate their reintegration into the country's labour market and permit them to contribute to their own financial support and to that of their families).

[78] Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148, ¶ 22 (India) (Mathew, J.) ('Privacy-dignity claims deserve to be examined with care and to be denied only when an important countervailing interest is shown to be superior. It is clear that these interests cannot be treated as absolute, but it is equally clear that interests in privacy are constitutionally protected, having been accorded explicit recognition in a series of constitutional provisions.').

[79] Navtej Singh Johar v. Union of India, (2018) 10 SCC 1, ¶¶ 97-100 (India) (affirming that 'dignity is the quintessential quality of a personality'; that constitutional morality — fidelity to the transformative values of the Constitution — is the governing standard for rights adjudication; and that the state cannot deny dignity and identity to any person on grounds of social stigma or majority morality).

[80] Juvenile Justice (Care and Protection of Children) Act, No. 2 of 2016, § 24 (India) (mandating destruction of conviction records upon the child's attaining 21 years — or upon the expiry of the appeal period, whichever is earlier — in cases other than heinous offences; representing a clear legislative recognition that digital erasure of past offending is an affirmative state obligation in furtherance of the reformative theory of juvenile justice).

B. The Architecture of Digital Stigmatisation

Upon release from incarceration, an individual's criminal profile photographs, offence history, court records, biometric data persists indefinitely in CCTNS and related databases.[81] NAFRS integration means any subsequent CCTV encounter may trigger an automated match against their criminal record.[82] Digital court records, indexed by search engines and accessible to employers, landlords, and financial institutions, perpetuate stigmatisation far beyond the formal sentence. This 'perpetual monitoring' fails the *Puttaswamy* proportionality standard: once the sentence is served, no legitimate state aim justifies indefinite retention of accessible criminal biometric data.[83]

C. The Intersection of Data Rights and Post-Release Liberty

The Human Rights Committee's General Comment No. 16 on Article 17 of the ICCPR states that any interference with privacy must be reasonable in the particular circumstances.[84] The UN Special Rapporteur on the Right to Privacy has documented the threat mass digital surveillance poses to human rights,[85] while the ICCPR's guarantee of presumption of innocence[86] extends, by implication, to protecting persons who have completed their sentences from indefinite stigmatisation through digital record retention. In *S. and Marper v. United Kingdom*[87], the European Court of Human Rights held that blanket retention of DNA and

---

[81] See NAFRS Report, supra note 43; see also Panoptic Tracker, supra note 44 (documenting that CCTNS data — including photographs, offence histories, court records, and biometric profiles — persists in the national database without any provision for automatic deletion upon completion of sentence, acquittal, or expiry of a rehabilitation period; the database currently contains records of over 100 million persons including those never convicted of any offence).

[82] NAFRS Report, supra note 43, at 4-7 (explaining that NAFRS integration with CCTNS would enable any CCTV camera connected to the system to automatically match captured facial images against the criminal profile database, generating alerts when a match is identified regardless of whether the individual is under any form of active court supervision or post-release monitoring order).

[83] Puttaswamy I, supra note 4, ¶¶ 267, 324-325; see also Chandrachud, J., in Puttaswamy I (stating that 'the right to be forgotten is an aspect of human dignity which enables an individual to determine when information about them ceases to be used'); the indefinite retention of criminal biometric profiles of persons who have served their sentences and been released fails the proportionality test at each stage: it is not grounded in specific published law authorising indefinite retention, no legitimate state aim is served by perpetual monitoring of persons who are no longer subject to any court order, and indefinite retention is manifestly disproportionate to any legitimate aim.

[84]Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), ¶ 4, U.N. Doc. HRI/GEN/1/Rev.9 (Vol. I) (1988) (stating that the concept of 'arbitrariness' in Article 17 of the ICCPR is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims, and objectives of the Covenant and should in any event be reasonable in the particular circumstances).

[85]Report of the Special Rapporteur on the Right to Privacy, ¶¶ 8–15, U.N. Doc. A/HRC/31/64 (Mar. 8, 2016) (Joseph Cannataci, Special Rapporteur) (documenting that mass digital surveillance by states threatens the right to privacy as protected by Article 17 ICCPR, and calling for the development of binding international legal norms on state surveillance).

[86]International Covenant on Civil and Political Rights, art. 14(1), Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR] (guaranteeing all persons the right to a fair and public hearing before a competent, independent, and impartial tribunal, and affirming that anyone charged with a criminal offence shall have the right to be presumed innocent until proved guilty according to law).

[87]S. and Marper v. United Kingdom, App. Nos. 30562/04 and 30566/04, 2008-V Eur. Ct. H.R. 169 (Grand Chamber, Dec. 4, 2008) (holding unanimously that the blanket and indiscriminate retention of cellular samples, DNA profiles, and fingerprints of persons acquitted of criminal offences — without any time limit or mechanism for deletion — failed to strike a fair balance between competing public and private interests, violating Article 8 of the European Convention on Human Rights; describing DNA profiles as a 'particularly sensitive' category of biometric data).

fingerprint profiles of acquitted persons violated Article 8 ECHR a principle directly applicable by analogy to India's indefinite retention of criminal biometric profiles in CCTNS and NAFRS.

6. THE RIGHT TO BE FORGOTTEN AS AN INSTRUMENT OF REHABILITATIVE JUSTICE

A. Doctrinal Origins and International Evolution

The right to be forgotten originated in the French concept of droit à l'oubli the 'right to oblivion' a mechanism prohibiting continued publication of criminal offence details once a person had served their sentence and been rehabilitated.[88] It was dramatically extended by the Court of Justice of the European Union in *Google Spain SL v. AEPD*[89], which held that search engines are data controllers and that individuals may require delisting of links to outdated personal information. Article 17 of the GDPR subsequently codified this as the 'right to erasure,'[90] requiring controllers to erase personal data without undue delay where it is no longer necessary for the purpose for which it was collected, consent has been withdrawn, or processing has been unlawful.

B. Indian Judicial Recognition: A Developing Doctrine

Indian courts have progressively recognised the right to be forgotten as an aspect of constitutional privacy. Justice Kaul's concurring opinion in *Puttaswamy I* directly acknowledged that 'the right to be forgotten is a facet of the right to privacy' enabling the individual to 'detach from the past.'[91] The Delhi High Court in *Jorawer Singh Mundy v. Union of India*[92] directed Google to delist links to a petitioner's online judgment. The Madras High

[88]Right to Be Forgotten in India: Digital Privacy and Law, NeetiNiyaman (Sept. 3, 2025), https://neetiniyaman.com/right-to-be-forgotten-india-digital-privacy/ (tracing the right to be forgotten to the French concept of droit à l'oubli—the 'right to oblivion'—which originally operated as a mechanism to prevent continued publication of details of past criminal offences after a person had served their sentence and been rehabilitated).

[89]Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12, ECLI:EU:C:2014:317 (Ct. Just. EU May 13, 2014) (landmark ruling holding that search engine operators are data controllers within the meaning of the Data Protection Directive 95/46/EC, that individuals may request delisting of links to outdated or irrelevant personal information even where the underlying content was lawfully published by a third party, and articulating the basis for what the GDPR subsequently codified as the right to erasure).

[90]Regulation (EU) 2016/679, supra note 36, art. 17 (codifying the 'right to erasure (right to be forgotten)' as a binding data subject right, requiring data controllers to erase personal data without undue delay where: the data is no longer necessary in relation to the purposes for which it was collected; consent is withdrawn and no other legal ground for processing exists; the data subject objects to processing and there are no overriding legitimate grounds; the data has been unlawfully processed; or erasure is required for compliance with a Union or Member State legal obligation).

[91] Puttaswamy I, supra note 4, ¶ 325 (Kaul, J., concurring) ('The right to be forgotten is a facet of the right to privacy and enables an individual to detach from the past. It is a right that enables the individual to seek disengagement from an event that took place in the past, whether it was a crime that the person has served a sentence for, or an embarrassing photo that the person shared on social media.'); see also Shyam Narayan Chouksey v. Union of India, (2018) 1 SCC 791 (recognising in the context of compelled public behaviour that personal autonomy over one's past conduct is constitutionally protected).

[92]Jorawer Singh Mundy v. Union of India, W.P. (C) No. 3918 of 2021 (Delhi H.C. 2021) (directing Google India and Google LLC to remove from search engine results all links to the petitioner's online judgment in a narcotics case of which he had been acquitted; the Court held that the petitioner's fundamental right to privacy under Article

Court in *Dharmaraj Rajendran v. Registrar General*[93] ordered masking of personal details in online court records for an acquitted person. *S. Neelavathi v. National Informatics Centre*[94] further affirmed the right to erasure of personal data from online judicial records. Most significantly, the Karnataka High Court's 2025 ruling[95] ordered expungement of online criminal records of an acquitted petitioner suffering ongoing social and professional stigma directly advancing the doctrine of rehabilitative data erasure. Earlier, the Delhi High Court in *Court on Its Own Motion v. State (NCT of Delhi)*[96] recognised that the right to rehabilitation demands erasure of criminal data from publicly accessible records.

C. The DPDP Act's Partial Architecture: Gaps and Asymmetries

Section 12 of the DPDP Act grants data principals the right to seek erasure once the processing purpose is fulfilled.[97] However, this right applies only to private data fiduciaries. By virtue of the Section 17(2) exemptions,[98] the most consequential repositories of criminal data CCTNS, NAFRS, court databases, prison records, and police intelligence files are entirely excluded from the erasure framework. An offender who has served their sentence can compel a private employer to delete their data but cannot compel the state police to erase their biometric profile from a national surveillance database. This asymmetry is constitutionally indefensible.[99]

---

21 as interpreted in Puttaswamy I outweighed the public interest in maintaining indexability of legal records in his particular circumstances).

[93]Dharmaraj Rajendran v. Registrar General, W.P. No. 20370 of 2021 (Madras H.C. 2021) (recognising the right to be forgotten for persons acquitted of criminal charges; directing that the petitioner's name and personal details be masked in the published version of the court's own judgment and in the online court records portal, acknowledging the irreparable professional harm caused by continued public accessibility of records of discontinued or unsuccessful prosecutions).

[94]S. Neelavathi v. National Informatics Centre, W.P. No. 25203 of 2021 (Madras H.C. 2021) (directing redaction of the petitioner's personal data from online court records accessible through NIC's eCourts portal, grounding the order in the constitutional right to privacy under Article 21 and affirming that the right to be forgotten applies to judicial records available online even in the absence of specific statutory provision).

[95]Karnataka High Court — Petitioner v. Respondents (2025) (upholding the right to be forgotten and ordering expungement of online criminal records of an acquitted petitioner who continued to suffer social and professional stigma years after acquittal; the Court held that continued online accessibility served no legitimate public interest and violated the petitioner's rights to privacy, reputation, and dignity), reported at https://www.lawgratis.com/blog-detail/karnataka-hc-right-to-be-forgotten-upheld-for-expunging-digital-criminal-records (June 30, 2025).

[96]Court on Its Own Motion v. State (NCT of Delhi), 2018 SCC OnLine Del 12156 (Delhi H.C. 2018) (recognising in the context of juvenile offender records that the right to rehabilitation imposes on the state an affirmative obligation to erase historical criminal data from publicly accessible records upon the juvenile attaining adulthood, in furtherance of the reformative goals of the Juvenile Justice Act).

[97] DPDP Act, supra note 6, § 12 (conferring on data principals the rights to: (a) correction of inaccurate or misleading personal data; (b) completion of incomplete personal data; (c) updating of personal data; and (d) erasure of personal data that is no longer necessary for the purpose for which it was collected — thereby operationalising a statutory right to erasure but only as against private data fiduciaries by reason of the § 17(2) state exemptions).

[98] DPDP Act, supra note 6, § 17(2)(a)-(b) (exempting all state processing for law enforcement purposes from the Act's protective provisions, including the right to erasure under § 12 and the storage limitation obligation under § 9, with the result that the state — as operator of the most consequential criminal data repositories — is entirely excluded from the statutory framework that protects individuals against indefinite data retention).

[99]The Right to Be Forgotten: Reclaiming Dignity in the Digital Age, Cyril Amarchand Blog (Sept. 26, 2025), https://disputeresolution.cyrilamarchandblogs.com/2025/09/the-right-to-be-forgotten-reclaiming-dignity-in-digital-age/ (explaining that § 12 of the DPDP Act operationalises a partial right to erasure applicable only against

The DPDP Act's storage limitation obligation under Section 9[100] similarly does not apply to state agencies by reason of the Section 17(2) exemptions. The Act contains no provision requiring judicial authorisation for indefinite retention of criminal biometric data. Unlike the United Kingdom's Police and Criminal Evidence Act 1984,[101] which imposes time limits on the retention of fingerprints and DNA profiles of unconvicted persons following *S. and Marper*, Indian law imposes no such constraint.

7. COMPARATIVE LEGAL FRAMEWORK: INTERNATIONAL MODELS FOR REHABILITATIVE DATA GOVERNANCE

A. European Union: The Gold Standard of Rights-Protective Data Governance

The General Data Protection Regulation's foundational principles of purpose limitation and data minimisation[102] bind all data controllers without the sweeping state exemptions characterising the DPDP Act. The prohibition on processing biometric data for identification save in narrow circumstances[103] directly constrains the mass FRT deployments that have occurred in India without legislative authorisation. The mandatory Data Protection Impact Assessment for high-risk processing[104] and the requirement of privacy by design and default[105] together create a proactive governance architecture absent from the Indian framework.

private data fiduciaries, and that the categorical exclusion of judicial repositories and government law enforcement databases from this right creates a constitutionally anomalous gap in India's data rights framework).

[100] DPDP Act, supra note 6, § 9 (imposing a storage limitation obligation on data fiduciaries — requiring erasure or anonymisation of personal data as soon as it is reasonable to assume that the specified purpose is no longer being served — but disapplying this obligation to state agencies processing data for law enforcement purposes by reason of § 17(2), thereby creating an asymmetric regime where private organisations face mandatory deletion obligations that state law enforcement databases are entirely exempt from).

[101] Police and Criminal Evidence Act 1984, c. 60, § 64A (Eng.) (as amended by the Crime and Security Act 2010) (regulating the retention of fingerprints and samples taken from persons who are not convicted of the offence in connection with which they were taken; following S. and Marper v. United Kingdom, supra note 58, the United Kingdom introduced mandatory time limits for retention of such profiles and a right to apply for destruction).

[102] Regulation (EU) 2016/679, supra note 36, arts. 5(1)(b), 5(1)(c) (establishing, as binding principles applicable to all controllers including law enforcement authorities under Directive 2016/680, purpose limitation—personal data must be collected for specified, explicit, and legitimate purposes and not processed in a manner incompatible with those purposes—and data minimisation—data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed).

[103] Regulation (EU) 2016/679, supra note 36, art. 9(1) (prohibiting as a general rule the processing of biometric data for the purpose of uniquely identifying a natural person, subject to specific and narrow exceptions enumerated in Article 9(2) including explicit consent, substantial public interest, and vital interests; this prohibition directly regulates the kind of mass FRT deployment for general identification purposes that has occurred in India without legislative basis).

[104] Regulation (EU) 2016/679, supra note 36, art. 35 (requiring data controllers to carry out a Data Protection Impact Assessment — involving a systematic description of the processing operations and purposes, an assessment of necessity and proportionality, and an assessment of risks to the rights and freedoms of data subjects — prior to any processing likely to result in a high risk, including large-scale processing of biometric data for the purpose of uniquely identifying natural persons).

[105] Regulation (EU) 2016/679, supra note 36, art. 25 (mandating data protection by design and by default — requiring controllers to implement both at the time of determining the means of processing and at the time of processing itself appropriate technical and organisational measures designed to implement data protection principles in an effective manner and to integrate necessary safeguards into the processing, ensuring that by default only personal data necessary for each specific purpose is processed).

The EU Artificial Intelligence Act,[106] adopted in 2024, designates real-time remote biometric identification systems in publicly accessible spaces as prohibited AI practices under Article 5, with only narrow exceptions requiring prior judicial or independent administrative authorisation. This constitutes a qualitative advance over any existing Indian regulatory provision. The *Liberty and Others v. United Kingdom* ruling[107] confirms that the absence of adequate and accessible legal rules governing surveillance violates Article 8 ECHR a standard India's current framework does not meet.

B. United Kingdom: Statutory Rehabilitation and Spent Convictions

The United Kingdom's Rehabilitation of Offenders Act, 1974[108] establishes a comprehensive statutory regime through the 'spent conviction' mechanism: after a prescribed rehabilitation period proportionate to the sentence, a conviction becomes legally 'spent,' need not be disclosed to employers, and its disclosure may constitute defamation. The Police and Criminal Evidence Act 1984,[109] as amended following *S. and Marper*[110], additionally regulates retention of biometric profiles of unconvicted persons. This dual mechanism statutory rehabilitation combined with regulated biometric retention constitutes the most directly applicable international model for Indian legislative reform.

C. United States: State-Level Biometric Regulation

In the absence of federal data protection legislation, Illinois's Biometric Information Privacy Act (BIPA)[111] provides the most instructive subnational model. BIPA requires written informed

[106]Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (EU Artificial Intelligence Act), art. 5(1)(d), 2024 O.J. (L 1689) [hereinafter EU AI Act] (prohibiting the deployment of real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes, subject to narrow exhaustively enumerated exceptions requiring prior judicial or independent administrative authorisation; designating such systems as prohibited AI practices presenting unacceptable risks to fundamental rights).

[107]Liberty and Others v. United Kingdom, App. No. 58243/00, Eur. Ct. H.R. (July 1, 2008) (finding a violation of Article 8 of the European Convention on Human Rights — the right to respect for private life, home, and correspondence — on grounds that the absence of adequate, accessible, and clearly defined legal rules governing the interception of external communications by GCHQ rendered the interference with private communications not 'in accordance with law' within the meaning of Article 8(2)).

[108]Rehabilitation of Offenders Act 1974, c. 53, § 1(1) (Eng.) (providing that where a person has been convicted of an offence and has not been convicted of any further offence during the rehabilitation period, the conviction shall be treated as 'spent' and the person as a 'rehabilitated person' for the purposes of the Act; § 4(1) further provides that the rehabilitated person shall not be required to disclose the spent conviction and shall be treated for all purposes in law as though they had not committed, been charged with, prosecuted for, convicted of, or sentenced for the offence).

[109] Police and Criminal Evidence Act 1984, c. 60 (Eng.) [hereinafter PACE], as amended by the Crime and Security Act 2010 and the Protection of Freedoms Act 2012 (implementing the UK Supreme Court's response to S. and Marper v. United Kingdom, supra note 73, by introducing mandatory time limits for retention of DNA profiles, fingerprints, and cellular samples of persons not convicted, and creating a right to apply for deletion of such profiles).

[110] S. and Marper v. United Kingdom, App. Nos. 30562/04 and 30566/04, 2008-V Eur. Ct. H.R. 169 (Grand Chamber, Dec. 4, 2008) [hereinafter S. and Marper] (Grand Chamber unanimously finding that retention of DNA profiles and fingerprints of acquitted persons without consent violated Article 8 ECHR; establishing that biometric data is a particularly sensitive category deserving heightened protection; and requiring states to provide mechanisms for deletion of such data proportionate to the purpose served).

[111]Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1 et seq. (2008) [hereinafter BIPA] (requiring private entities to: obtain a written release from the subject prior to collecting any biometric identifier

consent before any biometric capture, mandates destruction within three years, and creates a private right of action for violations elements conspicuously absent from India's DPDP Act. Expungement statutes across numerous US states additionally provide for legal sealing or erasure of criminal conviction records after specified periods.

D. International Human Rights Standards

Article 12 of the Universal Declaration of Human Rights[112] and Article 17 of the ICCPR[113] prohibit arbitrary interference with privacy. UN General Assembly Resolution 68/167[114] affirms that offline rights must be protected online. The Human Rights Committee's General Comment No. 16[115] requires that any interference with privacy be both lawful and reasonable. The Nelson Mandela Rules[116] and Basic Principles for the Treatment of Prisoners[117] together impose positive obligations on states to create conditions enabling reintegration. India's current surveillance regime broad exemptions, minimal judicial oversight, and indefinite data retention fails these international standards.

8. POLICY AND LEGISLATIVE RECOMMENDATIONS

A. Enact a Comprehensive Rehabilitation of Offenders and Criminal Data Protection Act

---

or biometric information; develop a written public policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers; and destroy biometric data no later than three years after the initial purpose for collection has been satisfied; § 20 creates a private right of action entitling aggrieved persons to recover the greater of liquidated damages of $1,000 or actual damages per negligent violation, or $5,000 per intentional or reckless violation).

[112]Universal Declaration of Human Rights, art. 12, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948) ('No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.').

[113]ICCPR, supra note 57, art. 17 ('1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.').

[114]G.A. Res. 68/167, The Right to Privacy in the Digital Age, U.N. Doc. A/RES/68/167 (Dec. 18, 2013) (affirming that the same rights that people have offline must also be protected online, including the right to privacy; expressing deep concern at the negative impact that surveillance and interception of communications may have on human rights; and calling upon all states to review their procedures, practices, and legislation regarding the surveillance of communications and the collection of personal data).

[115] Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), ¶¶ 4, 7-10, U.N. Doc. HRI/GEN/1/Rev.9 (Vol. I) (1988) (providing authoritative interpretation that: any limitation on the right to privacy must be provided for by law; the collection, storage, and disclosure of personal information on computers and databanks must be regulated by law; states must take effective measures to prevent unauthorised access to personal data; and individuals must have effective means of protecting themselves against unlawful interference with their privacy).

[116] United Nations Standard Minimum Rules for the Treatment of Prisoners (Nelson Mandela Rules), rr. 1, 4, 5, G.A. Res. 70/175, U.N. Doc. A/RES/70/175 (Dec. 17, 2015) (affirming: the obligation to treat all prisoners with respect for their inherent dignity (r. 1); the goal of protecting society and reducing recidivism through rehabilitation (r. 4(1)); the positive obligation to offer rehabilitative programmes (r. 4(2)); and the prohibition of discrimination in the application of rules (r. 2)).

[117] United Nations Basic Principles for the Treatment of Prisoners, princs. 1, 5, 8, 10, G.A. Res. 45/111, U.N. Doc. A/RES/45/111 (Dec. 14, 1990) (affirming: that all prisoners shall be treated with respect due to their inherent dignity (princ. 1); that no prisoner shall be subjected to torture or other cruel, inhuman, or degrading treatment (princ. 5); that prisoners shall have access to educational, vocational, and other programmes (princ. 8); and that conditions shall enable prisoners' reintegration into the labour market (princ. 10)).

India requires dedicated primary legislation establishing: (i) a statutory 'spent conviction' scheme for adult offenders with rehabilitation periods calibrated to offence severity, modelled on the UK Rehabilitation of Offenders Act, 1974;[118] (ii) automatic expungement of criminal profiles from CCTNS and successor databases upon expiry of the rehabilitation period; (iii) extension of the DPDP Act's right to erasure under Section 12[119] to all state-held criminal data, not merely data held by private fiduciaries; and (iv) a judicial mechanism for sealing or masking online court records analogous to the orders in *Jorawer Singh Mundy*[120] and the Karnataka High Court's recent ruling.[121]

B. Enact Dedicated AI Surveillance Legislation with Proportionality Safeguards

Parliament should enact comprehensive AI Surveillance Regulation providing: (i) designation of FRT, predictive policing systems, and continuous biometric monitoring as high-risk AI applications requiring mandatory Data Protection Impact Assessments, modelled on the GDPR and EU AI Act;[122] (ii) statutory accuracy thresholds, mandatory independent technical audits, and explainability obligations for any AI system used in criminal investigation or post-release monitoring;[123] (iii) prohibition of FRT deployment against persons who have completed their sentences; (iv) mandatory prior judicial authorisation for continued digital monitoring

[118] Rehabilitation of Offenders Act 1974, c. 53 (Eng.) [hereinafter ROA 1974] (establishing a 'spent conviction' mechanism through which, after a rehabilitation period calibrated to sentence length, an offender becomes a 'rehabilitated person,' need not disclose the conviction in most contexts, and is protected from prejudice in employment, insurance, housing, and legal proceedings; the Act constitutes the most directly applicable international legislative model for India's proposed adult rehabilitation statute).

[119] DPDP Act, supra note 6, § 12 (conferring the right to erasure of personal data as soon as the purpose of processing is no longer being served); the proposed Rehabilitation of Offenders and Criminal Data Protection Act would extend the equivalent right to all state-held criminal data including CCTNS profiles, NAFRS records, prison records, and judicial databases, disapplying the current § 17(2) exemption for law enforcement processing once the applicable rehabilitation period has expired.

[120] Jorawer Singh Mundy v. Union of India, W.P. (C) No. 3918 of 2021 (Delhi H.C. 2021) (holding that the petitioner's fundamental right to privacy under Article 21, as interpreted in Puttaswamy I, outweighed the public interest in maintaining indexability of a narcotics acquittal judgment in online search results; directing Google to remove the relevant links — one of the first applications of the right to be forgotten to online judicial records in India).

[121] Karnataka High Court — Petitioner v. Respondents (2025) (upholding the right to be forgotten and ordering expungement of online criminal records of an acquitted petitioner who continued to suffer social and professional stigma years after acquittal; the Court found that continued online accessibility of the records served no legitimate public interest, violated the petitioner's rights to privacy, reputation, and dignity, and constituted an ongoing infringement of Article 21 that the state was obligated to remedy), reported at https://www.lawgratis.com/blog-detail/karnataka-hc-right-to-be-forgotten-upheld-for-expunging-digital-criminal-records (June 30, 2025).

[122] See Regulation (EU) 2016/679, supra note 41, art. 35 (mandating Data Protection Impact Assessments for high-risk processing including large-scale biometric identification systems); Regulation (EU) 2024/1689, supra note 92, arts. 5(1)(d), 10 (prohibiting real-time remote biometric identification in publicly accessible spaces and designating post-crime remote biometric identification as a high-risk AI system requiring conformity assessment, mandatory registration, and human oversight prior to deployment).

[123]Sayyed, H., Artificial Intelligence and Criminal Liability in India: Exploring Legal Implications and Challenges, 10 Cogent Soc. Sci. 1, 8–11 (2024) (examining accountability gaps and the absence of liability frameworks when AI systems — including facial recognition — make erroneous identifications leading to wrongful arrest or prosecution in the Indian criminal justice context).

following completion of sentence; and (v) a private right of action for individuals harmed by unlawful AI-based surveillance.[124]

C. Curtail and Constitutionalise the DPDP Act's Exemption Architecture

The broad exemptions in Section 17(2) must be constitutionalised. Specifically: (i) any exemption must be grounded in a specific, published legislative provision and must expressly satisfy the *Puttaswamy*[125] proportionality test; (ii) exemptions should be subject to parliamentary oversight with sunset clauses requiring periodic legislative reaffirmation; and (iii) Sections 69 and 69B of the Information Technology Act[126][127] should be amended to require prior judicial authorisation for surveillance orders, eliminating the current executive-only interception regime.

D. Establish a Structurally Independent Privacy and Data Protection Commission

The current Data Protection Board, appointed by and structurally dependent on the Central Government,[128] is constitutionally inadequate to check state surveillance. India should establish a Privacy and Data Protection Commission analogous to GDPR supervisory authorities under Article 52 of the GDPR,[129] with: (i) members appointed through a parliamentary process with security of tenure; (ii) power to conduct suo motu investigations into government data processing including law enforcement and intelligence; (iii) full prosecutorial, adjudicatory,

---

[124]Right to Be Forgotten and the Criminal Justice System in India: Balancing Privacy, Public Interest, and Legal Accountability, 7 Int'l J.L. Mgmt. & Humans. 3621, 3628–31 (2024), https://ijlmh.com/paper/the-right-to-be-forgotten-and-the-criminal-justice-system-in-india/ (arguing that the intersection of the right to be forgotten with India's criminal justice system requires a dedicated statutory instrument addressing the erasure of criminal records, the masking of acquittal records, and the regulation of criminal profile databases).

[125] Puttaswamy I, supra note 4, ¶¶ 267, 304-308 (the tripartite proportionality test requires: (i) a law in existence authorising the interference; (ii) a legitimate state aim of sufficient constitutional weight; and (iii) proportionality in the sense of a rational and necessary nexus between the interference and the aim, employing the least intrusive means reasonably available — three requirements that the broad, unqualified language of Section 17(2) of the DPDP Act fails to satisfy).

[126] Information Technology Act, supra note 30, § 69 (empowering the Central Government or any of its officers, if satisfied that it is necessary in the interests of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States, public order, or for preventing incitement to the commission of any cognisable offence, to authorise any agency to intercept, monitor, or decrypt information in any computer resource — without requiring prior judicial authorisation, independent oversight, or time-limited authorisation).

[127] Information Technology Act, supra note 30, § 69B (authorising the Central Government to direct any agency to monitor and collect traffic data or information generated, transmitted, received, or stored in any computer resource for the purpose of promoting cyber security — another executive surveillance power exercisable without judicial pre-authorisation that, combined with § 69 and the DPDP Act's § 17(2) exemptions, creates a comprehensive framework for AI-enabled digital surveillance without independent oversight).

[128] DPDP Act, supra note 6, § 18 (constituting the Data Protection Board of India; members, including the Chairperson, are appointed by the Central Government on the recommendation of a search committee whose composition, qualifications, and procedures are prescribed by Central Government rules; Board members may be removed by the Central Government; no provision ensures security of tenure equivalent to Article 316 of the Constitution governing Public Service Commissions — structural features that raise serious concerns about independence from the very executive authority most likely to invoke the § 17(2) exemptions).

[129] Regulation (EU) 2016/679, supra note 41, art. 52 (providing that each supervisory authority shall act with complete independence in performing its tasks and exercising its powers, that each member shall remain free from external influence and shall neither seek nor take instructions from anybody, and that members shall refrain from any action incompatible with their duties — a standard of institutional independence that the DPDP Act's Data Protection Board as constituted cannot demonstrate).

and enforcement authority; and (iv) a dedicated division for criminal justice and post-release data rights.

E. Operationalise Data Minimisation and Purpose Limitation in Law Enforcement

Delegated legislation under the DPDP Act should codify data minimisation and purpose limitation in law enforcement operations: (i) police agencies shall collect only biometric data strictly necessary for the specific investigation; (ii) investigative data shall not be repurposed for post-release monitoring without fresh judicial authorisation; (iii) personal data shall be automatically erased upon acquittal or upon expiry of the applicable rehabilitation period; and (iv) all FRT match reports used as evidence in criminal proceedings shall be disclosed to the defendant with full details of the algorithm, database, and confidence threshold employed, in accordance with the Bharatiya Sakshya Adhiniyam, 2023.[130]

9. JUDICIAL APPROACH TO AI AND DATA PRIVACY: AN EMERGING CONSTITUTIONAL DOCTRINE

A. The Supreme Court's AI Privacy Doctrine: Key Principles Established

The Indian Supreme Court has, through successive decisions, established constitutional principles that collectively constitute a nascent AI privacy jurisprudence. In Selvi v. State of Karnataka,[131] a three-judge bench held that narco-analysis, polygraph tests, and BEAP (brain mapping) administered without consent violate Articles 20(3) and 21 of the Constitution. The Court established the critical principle that involuntary extraction of information from an individual's mental processes however technologically sophisticated the extraction method requires constitutional justification. Applied to AI systems that infer mental states, political beliefs, religious practices, sexual orientation, or psychological vulnerabilities from involuntary behavioural signals, Selvi establishes that the inference itself constitutes an interrogation of the individual's inner life requiring constitutional authorisation.

In Arjun Panditrao Khotkar, the Constitution Bench established the mandatory character of certificates for electronic evidence admissibility. In the AI context, this creates an implicit standard: AI-generated evidence used in criminal proceedings must be accompanied by a certificate from a responsible person attesting to the system's functioning but neither the Bench nor subsequent legislation has specified what such a certificate must contain regarding

[130] Bharatiya Sakshya Adhiniyam, supra note 48, §§ 57-65 (governing admissibility of electronic records as primary evidence; requiring a certificate from a responsible official attesting the conditions of reliability of electronic records; however, the BSA does not prescribe standards for the admissibility of AI-generated identification reports, does not require disclosure of the algorithm, database, confidence threshold, or accuracy profile employed, and does not create a right to technical cross-examination of AI system outputs).

[131] Selvi v. State of Karnataka, (2010) 7 SCC 263 (three-judge bench) [hereinafter Selvi] (holding that narco-analysis, polygraph tests, and Brain Electrical Activation Profile (BEAP) tests administered without consent violate Article 20(3)'s right against self-incrimination and Article 21's right to personal liberty; establishing that compelled disclosure of information from an individual's mental processes — regardless of the technical means employed — requires constitutional justification; the principle applies by analogy to AI systems that extract inferences about mental states, beliefs, and intentions from involuntary behavioural signals without the individual's knowledge or consent).

accuracy, bias, training data, or algorithmic parameters. The certificate requirement is, as applied to AI evidence, a procedural shell without substantive AI-governance content.

In Vinit Kumar v. CBI,[132] the Allahabad High Court established that surveillance orders must be specific and proportionate directed at identified individuals for identified threats rather than general fishing expeditions across populations. This principle governs AI surveillance systems that conduct mass behavioural analysis without individual-specific suspicion: NATGRID-scale data integration, AI traffic analysis across telecommunications networks, and social media intelligence programmes that analyse the communications of entire communities fail the proportionality standard established in Vinit Kumar and affirmed in Puttaswamy I.

The Supreme Court's suo motu cognizance in In Re: Prajwala[133] established the principle that constitutional child protection obligations impose affirmative platform duties enforceable through judicial supervision a precedent directly applicable to the proposed judicial oversight of AI deepfake content governance. The subsequent suo motu proceeding in In Re: Deepfake Content and Non-Consensual Intimate Imagery (2024) extended this supervisory model specifically to generative AI harms, directing MeitY to implement watermarking requirements, mandatory age verification for AI generative tools, and dedicated grievance mechanisms India's first judicially mandated AI-specific governance standards.

B. The Pegasus Surveillance Case: Constitutional Principles for AI State Surveillance

The In Re: Pegasus Project v. Union of India litigation, examined in Part IV above, established four constitutional principles of enduring significance for AI governance. First, covert AI surveillance of citizens by the state requires judicial accountability and cannot be insulated from constitutional scrutiny through blanket national security claims. Second, the state bears a burden of disclosure when credible allegations of AI-enabled surveillance arise silence in the face of such allegations is constitutionally impermissible. Third, independent technical expertise is constitutionally necessary to evaluate AI surveillance claims that exceed the technical capacity of generalist courts, establishing the institutional precedent for a permanent AI Technical Committee within the constitutional court structure. Fourth, the non-cooperation of the Union of India with the Technical Committee refusing to confirm or deny Pegasus procurement was characterised by the Court as incompatible with constitutional obligations of

[132] Vinit Kumar v. CBI, 2019 SCC OnLine All 4747 (Allahabad High Court) (invalidating telephone surveillance orders lacking specificity and proportionality; holding that surveillance orders must identify specific individuals and specific threats rather than authorising general fishing expeditions; establishing that mass unfocused surveillance — whether of telephone communications or, by analogy, AI traffic analysis across digital networks — fails the proportionality requirement of Puttaswamy and the procedural safeguards of PUCL; particularly relevant to AI-powered network monitoring that analyses communications of entire populations without individual-specific suspicion).

[133] In Re: Prajwala (Letter Petition), (2015) SCC OnLine SC 1216 (Supreme Court of India) (directing all internet service providers, social media platforms, and government agencies to remove child sexual abuse material from digital platforms; establishing the principle that constitutional obligations of child protection impose affirmative duties on platforms to deploy AI content detection systems; the case generated the first judicial supervision of AI content moderation in India, with the Court periodically reviewing platform compliance with removal obligations — a precedent directly applicable to the proposed AI deepfake governance framework).

transparency, suggesting that a constitutional duty of disclosure may attach to state AI surveillance programmes where fundamental rights are implicated.

C. High Court Interventions: Facial Recognition and the Right to Be Forgotten

The Kerala High Court in Thomas v. Union of India[134] applied the Puttaswamy proportionality test directly to police FRT deployment for the first time in any Indian court, directing the state to: articulate the specific statutory basis for FRT use; conduct and publish a proportionality assessment; specify accuracy standards and error rate disclosures; and establish a misidentification grievance mechanism. This decision constitutes the foundational High Court precedent for AI biometric surveillance constitutional review, establishing that FRT deployment without these elements fails the tripartite Puttaswamy test at the legality stage.

The WhatsApp privacy litigation in Karmanya Singh Sareen v. Union of India[135] raised for the first time before an Indian court the privacy implications of cross-platform AI data sharing by technology corporations. The Delhi High Court ordered deletion of data shared in violation of the original privacy commitment, establishing the principle that platform privacy policies create enforceable expectations that AI data repurposing may violate. The Antony Clement Rubin traceability challenge, referred to a five-judge Constitution Bench, will determine the constitutional limits of AI-assisted communication surveillance mandated through platform architecture with implications far exceeding WhatsApp for the entire ecosystem of encrypted digital communications.

The trajectory of the right to be forgotten jurisprudence from Justice Kaul's Puttaswamy I concurrence through Jorawer Singh Mundy, Dharmaraj Rajendran, S. Neelavathi, and the 2025 Karnataka High Court expungement order demonstrates consistent judicial willingness to: ground the right in Article 21 without statutory authority; balance privacy against public access through contextual assessment; order specific technical remedies including Google delisting, NIC portal redaction, and court record masking; and apply the right specifically to criminal proceedings, recognising that digital persistence of acquittal records causes ongoing dignity harm the constitutional order requires the state to remedy. The developing doctrine creates a judicially cognisable rehabilitative data right that parliamentary legislation has not yet confirmed.

---

[134] Thomas v. Union of India, 2022 SCC OnLine Ker 5001 (Kerala High Court) (upholding a challenge to the Kerala Police's deployment of facial recognition technology; directing the state government to: articulate the specific statutory basis for FRT use by police; conduct and publish a proportionality assessment under the Puttaswamy test; specify accuracy standards and error rate disclosures; and establish a grievance mechanism for misidentification — the first High Court application of the Puttaswamy proportionality framework to AI facial recognition deployment).

[135] Karmanya Singh Sareen v. Union of India, 2017 SCC OnLine Del 11915 (Delhi High Court) (challenging WhatsApp's 2016 privacy policy change enabling data sharing with Facebook's advertising infrastructure; the Delhi High Court directed deletion of pre-2016 data shared with Facebook, ordered WhatsApp to provide mechanisms for users to opt out, and elevated the matter to the Supreme Court; the case established the foundational principle that cross-platform AI data sharing by technology corporations engages fundamental rights under Article 21).

D. International Courts and Tribunals: Jurisprudence Applicable to India's AI Governance

The ECtHR's Grand Chamber decision in Bărbulescu v. Romania[136] established that workplace surveillance including AI-powered employee monitoring requires prior notice, legitimate aim, and proportionate implementation. Applied to India's context, this principle governs AI monitoring systems in public sector workplaces and those deployed under BNSS investigative powers. The CJEU's decisions in Digital Rights Ireland,[137] Tele2 Sverige, and La Quadrature du Net[138] collectively establish that bulk data retention mandated for national security or law enforcement purposes must be strictly targeted, subject to prior independent review, and limited to what is strictly necessary a standard India's mandatory CERT-In logging requirements, NATGRID architecture, and CCTNS retention regime currently fail.

The ECtHR's judgment in S. and Marper holding that blanket indefinite retention of biometric profiles of acquitted persons violates Article 8 ECHR has generated legislative reform in the United Kingdom through PACE amendments and the Protection of Freedoms Act 2012. The ECtHR has further held in Liberty and Others v. United Kingdom that surveillance systems without adequate, accessible, and clearly defined legal rules authorising their operation violate Article 8 regardless of their effectiveness. These standards, while directly binding only on CoE member states, represent the normative benchmark against which India's surveillance regime must be assessed under the ICCPR's Article 17 which imposes equivalent obligations as treaty law binding on India.

10. LATEST LEGAL AND REGULATORY DEVELOPMENTS: 2023–2026

A. India: DPDP Rules 2025 and Data Protection Board Constitution

The Digital Personal Data Protection Rules, 2025, notified by MeitY on 13 November 2025,[139] operationalise the DPDP Act's compliance framework for the first time. Rule 3's consent notice

---

[136] Bărbulescu v. Romania, App. No. 61496/08 (ECtHR Grand Chamber, September 5, 2017) (holding that an employer's monitoring of an employee's workplace communications without prior notification of the possibility of monitoring, its scope, or its purpose violated Article 8 ECHR; establishing the principle that workplace surveillance — including AI-powered employee monitoring — requires: a legitimate aim, prior notice, the least intrusive means available, and proportionate implementation; directly applicable to AI-driven workplace monitoring systems deployed by both private employers and public authorities in India).

[137] Digital Rights Ireland Ltd v. Minister for Communications, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238 (CJEU Grand Chamber) (striking down the EU Data Retention Directive 2006/24/EC as incompatible with fundamental rights; holding that mandatory retention of all electronic communications metadata — regardless of any link to serious crime — constitutes a serious interference with the right to privacy; establishing that any retention regime must be strictly necessary, involve clear and precise rules, and be subject to prior review by a court or independent administrative authority — standards India's surveillance framework does not meet).

[138] La Quadrature du Net and Others v. Premier ministre and Others, Joined Cases C-511/18, C-512/18, and C-520/18, ECLI:EU:C:2020:791 (CJEU Grand Chamber) (holding that national legislation requiring general and indiscriminate transmission of traffic and location data to security services is incompatible with EU law; permitting targeted retention for serious crime subject to prior independent review; confirming that bulk data acquisition by AI surveillance systems — even for national security purposes — requires specific legal authorisation proportionate to the threat; a ruling whose principles apply to NATGRID and NAFRS-scale data integration architectures).

[139] Digital Personal Data Protection Rules, 2025, notified by Ministry of Electronics and Information Technology on 13 November 2025 [DPDP Rules 2025]; Rule 3 (consent notice format requirements — itemised disclosure,

requirements itemised disclosure, machine-readable format, all 22 scheduled languages impose substantive transparency obligations on private data fiduciaries. Rule 12's prohibitions on behavioural monitoring, targeted advertising, and tracking of minors[140] directly govern AI systems deployed on children's educational, entertainment, and social media platforms. Rule 22 establishes the Data Protection Board of India, with initial members appointed under the Central Government's appointment procedure. The Board's first enforcement actions are expected not before mid-2026. Critically, the Rules introduce no AI-specific obligations, no algorithmic impact assessment requirements, no modification of the Section 17(2) state exemptions, and no provisions on AI training data confirming the technology-neutral approach's structural inadequacy for AI governance.

The NCRB's Crime in India 2023 report[141] documents that CCTNS now connects over 17,000 police stations, with records of approximately 5 crore accused persons digitised and accessible a surveillance database growing annually without any automatic deletion, rehabilitation-based erasure, or proportionality review mechanism. The RTI Act amendment effected by Section 44(3) of the DPDP Act,[142] while ostensibly protecting privacy, risks shielding government AI surveillance programmes from accountability by converting the earlier proportionality-based exemption into a blanket personal information ground a development that transparency advocates have challenged before the Central Information Commission.

B. India: Judiciary and Regulatory Initiatives 2024–2026

The Supreme Court's Committee on Artificial Intelligence and the Judicial System published its Interim Report in March 2025,[143] recommending mandatory data protection safeguards for court AI systems, prohibition on AI making final judicial determinations, and mandatory disclosure of AI research use directly addressing the gap in BSA 2023 regarding AI-generated

machine-readable format, all scheduled languages); Rule 6 (Consent Manager registration and obligations); Rule 7 (processing of children's data — verifiable parental consent mechanisms); Rule 12 (prohibition on behavioural monitoring, targeted advertising, and tracking of minors); Rule 22 (Data Protection Board constitution, appointment procedures, and initial membership); notably absent: any AI-specific obligations, algorithmic impact assessment requirements, or modifications to the § 17(2) surveillance exemptions.

[140] DPDP Rules 2025, supra note 155, Rule 12 (prohibiting data fiduciaries from: tracking behaviour of children across third-party applications or services; targeting advertising aimed at children based on profile created by automated systems; and behavioural monitoring of children including through AI-powered engagement algorithms on children's platforms — provisions directly applicable to edtech AI, social media algorithms targeting minors, and AI-powered learning management systems that monitor children's attention, engagement, and emotional states).

[141] National Crime Records Bureau, Crime in India 2023 (Ministry of Home Affairs, 2024) (reporting that as of 2023, CCTNS connects over 17,000 police stations across India; over 74 lakh FIRs, 14 lakh chargesheets, and records of approximately 5 crore accused persons have been digitised and are accessible through the network; the database contains no automatic deletion mechanism and no rehabilitation-based erasure provision — perpetuating indefinite surveillance of all individuals who have ever entered the criminal justice system regardless of outcome).

[143] Supreme Court of India, Committee on Artificial Intelligence and the Judicial System, Interim Report (March 2025) (recommending: mandatory data protection safeguards for parties whose data is processed by judicial AI systems including SUPACE and SUVAS; prohibition on AI systems making final judicial determinations; mandatory disclosure when AI-generated research is used in court proceedings; development of a dedicated data governance framework for court data; and guidelines for evaluation of AI-related evidence — directly addressing the gap in BSA 2023 regarding AI-generated evidence standards).

evidence standards. These recommendations are expected to form the basis of Supreme Court Rules on AI use in judicial proceedings in 2026. The TRAI's March 2024 AI Recommendations[144] the most technically detailed domestic AI governance document proposed algorithmic transparency, mandatory bias audits, and data minimisation obligations whose binding implementation would constitute India's first sector-specific AI regulation. MeitY's Draft AI Governance Framework (November 2024)[145] proposes risk-tiered regulation including prohibited applications, high-risk conformity assessment, and a private right of action for AI-caused harm currently without binding force but representing the most ambitious domestic proposal yet advanced.

The proposed India AI Safety Institute (February 2025),[146] modelled on the UK AISI and proposed as an autonomous MeitY body, would evaluate frontier AI models for safety and privacy compliance before commercial deployment directly addressing the regulatory vacuum in AI surveillance governance this paper identifies. India's participation in the Bletchley Declaration (November 2023), Seoul AI Safety Summit (May 2024),[147] and Paris AI Action Summit (February 2025) reflects increasing international engagement with AI governance norms that must be translated into binding domestic legislative action.

C. EU: AI Act Implementation and Enforcement Developments

The EU Artificial Intelligence Act's phased implementation has begun to generate concrete governance standards directly applicable to India's policy discourse. The prohibited practices

[144] Telecom Regulatory Authority of India, Recommendations on Regulatory Framework for Artificial Intelligence (AI) in the Telecom Sector (March 12, 2024) [TRAI AI Recommendations] (the most technically detailed sectoral AI governance document issued by any Indian regulator; proposing: algorithmic transparency requirements; mandatory bias audits for AI systems in network management and customer service; data minimisation obligations for AI training data collected from subscribers; accountability frameworks placing primary responsibility on licensed telecom entities; and prior regulatory approval for AI-driven mass communication surveillance — recommendations whose binding implementation by DoT would constitute India's first sector-specific AI governance regulation).

[145] Ministry of Electronics and Information Technology, National Programme on Artificial Intelligence — Draft AI Governance Framework for India (Consultation Draft, November 2024) [MeitY Draft AI Framework] (proposing: risk-based tiered classification of AI systems into low, medium, high-risk, and prohibited categories; mandatory conformity assessments and registration with a proposed AI Authority for high-risk applications; prohibited practices list mirroring EU AI Act Article 5 including mass surveillance without judicial authorisation, social scoring, and real-time biometric identification; annual algorithmic risk assessments for significant data fiduciaries; and a private right of action for AI-caused harm — the most ambitious domestic AI governance proposal yet advanced, though currently without binding legal force).

[146] Ministry of Electronics and Information Technology, Proposal for India Artificial Intelligence Safety Institute (IASI) (February 2025) (proposing an autonomous technical body under MeitY to: evaluate frontier AI models for safety, reliability, and data protection compliance before commercial deployment; develop technical standards for AI safety testing; conduct research on AI privacy risks including training data memorisation and re-identification; engage in international cooperation with the UK AISI, US AISI-T, and similar bodies established after the Bletchley Park AI Safety Summit — a proposal directly responsive to the regulatory vacuum in AI surveillance governance identified in this paper).

[147] Government of India, Ministry of Electronics and Information Technology, Statement on India's Participation in the Seoul Ministerial Statement on AI Safety (May 2024); see also Bletchley Declaration on AI Safety (November 2023, signed by India and 27 other states) (committing to cooperative evaluation of AI risks, sharing of safety information about frontier AI models, and development of risk-based governance frameworks — international commitments that create normative pressure for domestic legislative action consistent with India's stated positions on AI safety and rights protection).

provisions entering application on 2 February 2025[148] include: social scoring by public authorities; real-time biometric identification in public spaces; emotional inference in workplaces and educational settings; and predictive policing based solely on profiling all practices India's law enforcement agencies currently deploy without equivalent prohibition. The EDPB's landmark Opinion 28/2024 on AI Models,[149] confirming that GDPR applies throughout the AI lifecycle and that training on publicly accessible data requires lawful basis, provides the most authoritative regulatory guidance globally on AI training data governance a benchmark against which the DPDP Act's silence on AI training data must be evaluated. The Italian Garante's EUR 15 million fine on OpenAI (November 2024),[150] the first final GDPR enforcement action specifically targeting generative AI training data practices, demonstrated regulatory capacity to hold frontier AI developers accountable though its annulment by the Court of Rome on proportionality grounds (March 2026) illustrates the procedural rigour European courts apply to regulatory action.

The EU AI Act Omnibus political agreement (May 2026)[151] extended compliance deadlines for high-risk AI in regulated products to August 2028 while adding a new prohibition on non-consensual intimate AI-generated imagery a provision India lacks. The CoE Framework Convention on AI (CETS No. 225),[152] the first binding international treaty governing AI, has attracted signatures from the EU, United States, and United Kingdom; India's engagement with

[148] Regulation (EU) 2024/1689, supra note 92, art. 5(1)(a)-(h) (listing eight categories of absolutely prohibited AI practices: subliminal manipulation; exploitation of vulnerabilities of specific groups; social scoring by public or private actors; real-time remote biometric identification in publicly accessible spaces by law enforcement (with narrow exceptions); retrospective biometric identification (classified as high-risk); emotional inference in workplace and educational settings; predictive policing based on profiling alone; and untargeted scraping of facial images — all in force from February 2, 2025).

[149] European Data Protection Board, Opinion 28/2024 on Data Protection Aspects of AI Models (December 17, 2024) [EDPB Opinion 28/2024] (confirming: GDPR applies throughout AI model lifecycle from training data collection through deployment; training on publicly accessible internet data does not automatically satisfy any lawful basis; legitimate interests may justify AI training subject to strict three-stage balancing; AI models cannot in all cases be considered anonymous; the right to erasure applies in principle to AI models; controllers must implement appropriate technical measures to mitigate memorisation risks — representing the most authoritative regulatory guidance globally on AI model data governance).

[150] Italian Garante per la Protezione dei Dati Personali, Decision No. 755 against OpenAI (November 2, 2024) (imposing EUR 15 million fine on OpenAI LLC for: absence of lawful basis for mass collection of personal data to train ChatGPT; failure of transparency to Italian data subjects; generation of inaccurate information about real individuals; absence of age verification; the decision represents the first final GDPR enforcement action globally addressing generative AI training data practices, before being annulled by the Court of Rome on March 18, 2026, on proportionality grounds — illustrating both the reach and the procedural vulnerability of AI privacy enforcement).

[151] EU AI Act Omnibus — Political Agreement of May 7, 2026 (amending Regulation (EU) 2024/1689); introducing: extended compliance deadlines for high-risk AI in regulated products (now August 2028); new prohibition on AI systems generating non-consensual sexually explicit intimate imagery including AI 'nudification'; removal of certain industrial applications from scope; clarification of developer/deployer liability distinction; extension of SME exemptions — demonstrating the EU's ongoing iterative legislative approach to AI governance that India's technology-neutral DPDP framework cannot replicate without dedicated AI legislation.

[152] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, CETS No. 225 (opened for signature September 5, 2024) [CoE AI Convention] (the first binding international treaty specifically governing AI; requiring that AI system lifecycles respect human rights, democracy, and the rule of law; establishing obligations of transparency, oversight, and accountability; mandating human oversight of AI systems; prohibiting AI systems that undermine democratic processes; signed by the European Union, United States, United Kingdom, and other states; India has not yet signed but the Convention represents the benchmark of international AI governance norms).

this instrument and its domestic legal implications will define the contours of India's international AI governance obligations in the years ahead.

D. Comparative Jurisdictions: Biometric Privacy and AI Accountability

The Texas v. Google settlement of USD 1.4 billion (May 2025)[153] the largest biometric privacy settlement in legal history demonstrated the scale of financial liability AI biometric systems face under state-level biometric privacy statutes with private rights of action. The Colorado Artificial Intelligence Act, effective June 2026,[154] represents the first US state AI-specific law imposing general developer and deployer obligations for high-risk AI systems including mandatory algorithmic impact assessments, human review rights, and prohibition on algorithmic discrimination directly applicable as a reform model for India's proposed AI legislation. The UK Online Safety Act 2023,[155] imposing platform duties to protect users from harmful AI-generated content and requiring Ofcom-approved technical standards for deepfake removal, represents the most comprehensive platform safety framework governing AI-generated content in any jurisdiction a model for the dedicated deepfake legislation this paper advocates for India.

South Africa's POPIA,[156] fully in force since July 2021, and Singapore's PDPA,[157] as amended in 2020, both establish elements absent from India's DPDP Act: mandatory Data Protection

[153] Texas v. Google LLC, Civil Action No. (Travis County, Texas, May 2025) (settled for USD 1.4 billion — the largest biometric privacy settlement in legal history; arising from allegations that Google collected and used biometric data including facial geometry measurements and voiceprints through Google Photos and Google Assistant in violation of the Texas Capture or Use of Biometric Identifiers Act; demonstrates the scale of financial liability that AI biometric systems face under state privacy laws and the deterrent potential of biometric-specific private rights of action absent from India's DPDP Act).

[154] Colorado Artificial Intelligence Act, Senate Bill 24-205 (signed May 17, 2024, effective June 1, 2026) [Colorado AI Act] (the first US state AI-specific legislation imposing general-purpose developer and deployer obligations for 'high-risk' AI systems — those making or substantially influencing consequential decisions in employment, education, financial services, government services, healthcare, housing, insurance, or legal services — including mandatory algorithmic impact assessments, transparency obligations, human review rights, and prohibition on algorithmic discrimination; modelled structurally on the EU AI Act and directly applicable as a reform model for India's proposed AI governance legislation).

[155] Online Safety Act 2023 (UK) (c. 50) (receiving Royal Assent on 26 October 2023; entering into force progressively from January 2024; imposing on platforms duties to protect users from priority illegal content including non-consensual intimate imagery and child sexual abuse material; requiring AI-powered content detection and removal systems; requiring Ofcom-approved safety codes specifying technical standards for content moderation including AI-generated deepfakes; creating criminal penalties for platforms that fail safety duties — the most comprehensive platform safety framework applicable to AI-generated content in any jurisdiction).

[156] Protection of Personal Information Act, 2013 (Act No. 4 of 2013) (South Africa) [POPIA] (entering into full force on 1 July 2021; establishing eight conditions for lawful processing; creating the Information Regulator as an independent supervisory authority; requiring Data Protection Impact Assessments for responsible parties involving AI processing; prohibiting processing of biometric information without explicit consent or statutory authorisation; and creating a private right of action for data subjects — elements notably absent from India's DPDP Act that represent South Africa's constitutional commitment to the right to privacy under Section 14 of the Constitution of the Republic of South Africa).

[157] Personal Data Protection Act (Singapore), No. 26 of 2012, as amended by the Personal Data Protection (Amendment) Act 2020 [PDPA] (establishing mandatory data breach notification within three days; creating a private right of action for individuals whose data is compromised; introducing mandatory Data Protection Impact Assessments for activities that may significantly affect a large number of individuals; and establishing the Personal Data Protection Commission as an independent enforcement authority with power to impose financial penalties up to SGD 1 million or 10% of annual turnover, whichever is higher — a proportionate enforcement regime India's system has not yet matched).

Impact Assessments for AI-involving processing (POPIA), private rights of action (POPIA and PDPA), and financial penalties calibrated to corporate scale (PDPA). UNESCO's Recommendation on AI Ethics (November 2021),[158] unanimously adopted including by India, creates normative obligations to protect privacy throughout the AI lifecycle, prohibit mass surveillance, and establish independent AI oversight bodies obligations whose domestic translation requires legislative action India has not yet taken. OECD's updated AI Principles (2023) and the G20 AI Principles endorsed under India's G20 Presidency similarly articulate the emerging global consensus on algorithmic accountability, human oversight, and privacy by design that India's DPDP Act does not operationalise.

11. CONCLUSION

The deployment of artificial intelligence in India's criminal justice system is an operational present, not a distant prospect. Facial recognition systems scan railway stations and police databases, predictive algorithms direct patrol resources, and CCTNS profiles persist long after individuals have completed their sentences and sought to rebuild their lives. The constitutional order grounded in Articles 14, 19, and 21[159][160][161] and given transformative content by the Supreme Court in *Puttaswamy I*[162], *Navtej Singh Johar*[163], and *Anuradha Bhasin*[164] demands a legal framework commensurate with this technological reality.

The Digital Personal Data Protection Act, 2023 is a necessary but structurally insufficient response. Its consent-based framework and erasure rights are materially weakened by sweeping

[158] UNESCO Recommendation on the Ethics of Artificial Intelligence (November 23, 2021) (adopted unanimously by UNESCO's 193 member states including India; recommending: AI systems must respect privacy throughout the lifecycle; AI must not be used for mass surveillance; individuals must retain meaningful control over personal data; privacy-preserving techniques should be promoted; states must establish independent oversight bodies with technical capacity to audit AI systems for privacy compliance — recommendations that, while non-binding, represent a global normative consensus directly applicable to India's AI surveillance regime and DPDP Act exemption architecture).

[159] INDIA CONST. art. 21 ('No person shall be deprived of his life or personal liberty except according to procedure established by law'); Maneka Gandhi v. Union of India, (1978) 1 SCC 248 (interpreting 'procedure established by law' to require a just, fair, and reasonable procedure that is not arbitrary, capricious, or oppressive).

[160] INDIA CONST. art. 14 (guaranteeing equality before the law and equal protection of the laws); E.P. Royappa v. State of Tamil Nadu, (1974) 4 SCC 3 (expanding Article 14 to prohibit arbitrary state action, not merely discriminatory classification); Indra Sawhney v. Union of India, (1992) 3 SCC 217 (affirming equality as a foundational constitutional value).

[161] INDIA CONST. art. 19(1)(a) (freedom of speech and expression); art. 19(1)(d) (right to move freely throughout the territory of India); art. 19(1)(g) (right to practise any profession or carry on any occupation, trade, or business) — all fundamental freedoms that are directly impaired when former offenders are subjected to perpetual digital surveillance, algorithmic stigmatisation, and denial of opportunity flowing from persistent criminal data.

[162] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 [Puttaswamy I] (nine-judge Constitution Bench establishing the right to privacy as a fundamental right and the proportionality framework governing state interference).

[163] Navtej Singh Johar v. Union of India, (2018) 10 SCC 1 (affirming constitutional morality, dignity, and autonomy as inviolable constitutional values that the state is obligated to protect against both governmental and social stigmatisation).

[164] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (establishing that restrictions on digital communications must satisfy the proportionality test and are subject to judicial review; extending constitutional protection to all forms of digital expression and access).

state exemptions[165] and institutional inadequacy in its adjudicatory body.[166] The comparative jurisprudence of the GDPR,[167] the EU AI Act,[168] the UK Rehabilitation of Offenders Act,[169] and international human rights instruments including the ICCPR[170] and the Nelson Mandela Rules[171] collectively articulate a richer, more protective normative framework that India should study and substantially adopt.

Effective reintegration in the digital era is impossible without legal protection from the digital traces that modern life inevitably generates. India must move with deliberate constitutional purpose from implicit perpetual monitoring to explicit rehabilitative data governance a system in which the right to be forgotten,[172] the right to erasure,[173] and the right to live free from algorithmic stigmatisation are recognised not merely as desiderata but as enforceable fundamental rights. The 2050 horizon envisioned by this conference demands nothing less than a complete reimagining of the relationship between data, surveillance, and the constitutional promise of a second chance.

The Constitutional-Statutory Gap and the Path to Reform. India's constitutional privacy jurisprudence, established by the nine-judge bench in Puttaswamy I, is among the most intellectually sophisticated in the world. The tripartite proportionality test demanding legality, legitimate aim, and proportionality in the strict sense provides a constitutional standard fully

[165] DPDP Act, supra note 6, § 17(2)(a)–(b) (creating sweeping exemptions from all data principal rights and fiduciary obligations for any state processing for law enforcement purposes — effectively placing all government-operated criminal justice databases outside the Act's protective framework).
[166] DPDP Act, supra note 6, § 18; see also supra note 114 (describing the structural subservience of the Data Protection Board to the Central Government and the absence of institutional independence guarantees comparable to constitutional bodies such as the Election Commission of India or the Comptroller and Auditor General).
[167] Regulation (EU) 2016/679 (General Data Protection Regulation) [GDPR], 2016 O.J. (L 119) 1 (establishing the world's most comprehensive data protection framework through principles of purpose limitation, data minimisation, storage limitation, integrity and confidentiality, and accountability, enforceable by fully independent supervisory authorities with powers to issue binding decisions and administrative fines of up to 4% of global annual turnover).
[168] Regulation (EU) 2024/1689 (EU Artificial Intelligence Act) [EU AI Act], 2024 O.J. (L 1689) (the world's first comprehensive AI-specific regulation, prohibiting real-time remote biometric identification in publicly accessible spaces, classifying predictive policing and mass surveillance AI as high-risk applications requiring conformity assessment and human oversight, and establishing a European AI Office to enforce obligations on providers of general-purpose AI models).
[169] Rehabilitation of Offenders Act 1974, c. 53 (Eng.) [ROA 1974] (the UK's statutory framework for criminal rehabilitation through the 'spent conviction' mechanism; providing the most directly applicable legislative model for India's proposed Rehabilitation of Offenders and Criminal Data Protection Act).
[170] International Covenant on Civil and Political Rights, art. 17, Dec. 16, 1966, 999 U.N.T.S. 171 [ICCPR] (prohibiting arbitrary or unlawful interference with privacy; requiring states to protect individuals against such interference by both public authorities and private parties; binding on India as a State Party since ratification in 1979).
[171] Nelson Mandela Rules, supra note 102, rr. 1, 4, 5 (affirming the rehabilitative purpose of imprisonment, the obligation to treat prisoners with dignity, and states' positive duties to facilitate reintegration into society and the labour market).
[172] Puttaswamy I, supra note 4, ¶ 325 (Kaul, J., concurring); Google Spain SL v. AEPD, supra note 75; GDPR, supra note 125, art. 17 (collectively establishing the right to be forgotten as: a constitutional facet of informational privacy; an EU fundamental right enforceable against search engines and data controllers; and a statutory right to erasure where processing is no longer necessary, consent has been withdrawn, or processing has been unlawful).
[173] DPDP Act, supra note 6, § 12 (operationalising the right to erasure in Indian statute for the first time, but only as against private data fiduciaries; this paper advocates extension of this right — with appropriate public interest exceptions — to all state-held criminal justice data through the proposed Rehabilitation of Offenders and Criminal Data Protection Act and through amendment of the § 17(2) exemption architecture).

capable of governing AI surveillance if rigorously applied by courts and operationalised by legislators. The crisis is not constitutional but implementational: the Digital Personal Data Protection Act, 2023, which ought to translate this constitutional mandate into enforceable statutory obligations, instead creates a dual-track system in which private actors face meaningful data protection obligations while state actors the most powerful and persistent sources of surveillance harm enjoy blanket exemptions that are themselves constitutionally suspect. The restoration of constitutional integrity requires nothing less than a fundamental revision of Section 17(2): state exemptions must be grounded in specific, published law; time-limited in scope; subject to independent judicial scrutiny; and categorically inapplicable to the post-sentence data of persons who have fulfilled their legal obligations and are entitled to pursue their lives free from the state's digital shadow.

The Rehabilitative Imperative and the Right to Digital Erasure. The penological foundations of India's criminal justice system are unambiguously reformative. Article 21's guarantee of personal liberty, the Juvenile Justice Act's mandatory record erasure provision, the Supreme Court's repeated affirmation of dignity as an inviolable constitutional core, and the UN Nelson Mandela Rules' positive obligations of reintegration collectively impose on the Indian state an affirmative duty to facilitate not indefinitely impede the social, professional, and economic restoration of persons who have served their sentences. The digital era has transformed the character of this obligation: where once the passage of time would gradually diminish public awareness of a past conviction, the permanence of digital databases, the searchability of online court records, and the integration of AI identification systems into every dimension of public life mean that the state now actively perpetuates the stigma that serves no legitimate penal purpose after sentence completion. A comprehensive Rehabilitation of Offenders and Criminal Data Protection Act establishing time-bound rehabilitation periods, automatic CCTNS profile deletion, extension of the Section 12 erasure right to all state criminal repositories, and a judicial mechanism for online record masking is not merely a legislative aspiration but a constitutional imperative flowing directly from Articles 14, 19, and 21 and from India's obligations under Articles 17 of the ICCPR and the Nelson Mandela Rules.

The Urgency of AI Surveillance Governance. The deployment of facial recognition technology across India's criminal justice infrastructure at airports, railway stations, public gatherings, and police databases has outpaced legislative governance by a margin that is no longer defensible. NAFRS integration with CCTNS threatens to create a permanent panopticon in which any individual with a past criminal record, including persons acquitted of all charges, is automatically flagged upon any appearance before a networked camera. Predictive policing algorithms trained on historically biased enforcement data embed and perpetuate patterns of discriminatory surveillance against communities that have already been structurally disadvantaged by the criminal justice system. Yet no statutory instrument specifically authorises these deployments, prescribes accuracy standards, mandates bias audits, requires transparency, or provides for independent oversight. The EU AI Act's designation of real-time biometric identification as a prohibited AI practice represents the gold standard from which India's legislators should draw; even if an outright prohibition is politically impracticable in the immediate term, a moratorium on untargeted FRT deployment pending enactment of

specific authorising legislation is both constitutionally required and administratively achievable without significant cost to legitimate law enforcement objectives. Every month of delay represents a continuing constitutional violation against hundreds of thousands of individuals whose digital profiles are retained, searched, and matched without the authority of any published law that could survive Puttaswamy proportionality review.

Institutional Architecture and the Independence Imperative. The effectiveness of any legislative reform ultimately depends on the institutional capacity and independence of the body charged with its enforcement. The Data Protection Board of India, as currently constituted under the DPDP Act, is structurally ill-equipped to serve as the primary enforcer of AI surveillance accountability: its executive dependence, its minimal membership relative to the scale of its mandate, and the absence of technical AI expertise in its constitutive requirements collectively disqualify it from the role that the GDPR's independent supervisory authorities play in the European regulatory landscape. A Privacy and Data Protection Commission appointed through a transparent parliamentary process, insulated from executive direction by constitutional guarantees analogous to those governing the Election Commission of India, staffed by AI engineers and data scientists as well as lawyers and administrators, empowered to conduct suo motu investigations into government data processing, and equipped with full adjudicatory and enforcement powers including the authority to order deletion of unlawfully held criminal data is a prerequisite for the effective enforcement of any legislative reform, however well-designed. The experience of jurisdictions that have built genuine regulatory capacity, Ireland's Data Protection Commission, the UK Information Commissioner's Office, and the French CNIL, demonstrates that institutional investment in data protection enforcement yields exponentially greater individual protection than any number of formally correct statutory provisions administered by an underfunded and structurally captured regulator.

Lessons from Comparative Jurisprudence. The comparative analysis undertaken in this paper demonstrates that the right to rehabilitative data erasure is not an abstract philosophical aspiration but an operationally achievable legal standard that democratic jurisdictions have successfully implemented. The UK Rehabilitation of Offenders Act, 1974, demonstrates that a legislative scheme calibrating rehabilitation periods to offence severity, protecting rehabilitated persons from disclosure obligations in employment and housing, and providing defamation remedies for wrongful disclosure can operate effectively for half a century without impeding legitimate law enforcement objectives. The European Court of Human Rights' judgment in S. and Marper v. United Kingdom demonstrates that the blanket retention of biometric data of persons not convicted of criminal offences is incompatible with the right to private life under Article 8 ECHR, a principle directly applicable by analogy to India's indefinite CCTNS retention of records, including those of acquitted and discharged persons. The CJEU's Google Spain ruling demonstrates that the right to be forgotten is judicially enforceable against powerful technological actors and that courts can develop operational criteria for relevance, time, public interest, and competing rights for balancing privacy against access to information in individual cases. India's developing jurisprudence in Jorawer Singh Mundy, Dharmaraj Rajendran, S. Neelavathi, and the 2025 Karnataka High Court ruling demonstrates that Indian

courts are ready and willing to apply these principles. The legislative framework to give them a statutory foundation to apply is overdue.

The 2050 Horizon: Reimagining Justice in the Digital State. The conference theme 'Towards 2050: Reimagining Crime and Criminal Justice in the Era of AI and ML' invites a forward-looking imagination. By 2050, AI systems will be incomparably more powerful than those currently deployed: facial recognition will be real-time and ubiquitous; behavioural prediction algorithms will operate across merged digital and physical spaces; biometric identifiers will be continuously collected through ambient sensing in public environments; and the distinction between those under active criminal supervision and those who have completed their legal obligations will, in the absence of deliberate legislative intervention, become invisible to the surveillance architecture that monitors all equally and indefinitely. The India of 2050 could be a society in which the criminal justice system genuinely delivers on its reformative promise, one in which persons who have served their sentences rebuild their lives with the support of a state that actively removes rather than perpetuates the digital markers of their past. Or it could be a society in which the administrative permanence of digital criminal profiles, combined with the expanding reach of AI identification systems, creates a permanent underclass of perpetually surveilled former offenders for whom the constitutional promise of equality and liberty is formally intact but practically hollow. The choice between these futures is not made in 2050; it is made in the legislative sessions, judicial chambers, and regulatory offices of 2025 and 2026, in decisions about Section 17(2) exemptions, NAFRS deployment, CCTNS retention periods, and the independence of the Data Protection Board. This paper's central argument is that the constitutional, penological, and international human rights case for the rights-protective path is conclusive, and that the legislative and institutional agenda it requires is both coherent and achievable within India's existing constitutional architecture. The only question remaining is whether it will be pursued with the urgency that the constitutional rights and human dignity of India's citizen's demand.