INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

AI, SURVEILLANCE, AND THE RIGHT TO PRIVACY: AN INDIAN CONSTITUTIONAL PERSPECTIVE

AUTHORED BY - ABHISHEK SINGH
& DR. SANJAY KULSHRESHTHA

ABSTRACT

India's accelerating integration of artificial intelligence into public surveillance infrastructure—notably facial recognition systems, predictive policing algorithms, and mass data profiling—fundamentally undermines constitutional privacy protections enshrined under Article 21. Despite the Supreme Court's landmark affirmation of privacy as an intrinsic right in Justice K.S. Puttaswamy v. Union of India (2017), pervasive governance deficiencies enable systematic violations: surveillance technologies routinely operate without parliamentary authorization, judicial oversight, or accountability mechanisms, directly contravening Puttaswamy's proportionality framework of legality, legitimate aim, and necessity. This paper identifies three critical constitutional fault lines: First, the consistent non-implementation of Puttaswamy's safeguards permits extra-legal biometric harvesting through projects like the National Automated Facial Recognition System (NAFRS). Second, algorithmic opacity in "black box" systems institutionalizes discrimination against Scheduled Castes/Tribes, religious minorities, and women—violating equality guarantees under Articles 14–15 through biased outcomes documented in criminal justice deployments. Third, India's regulatory divergence from emerging global standards (particularly the GDPR's purpose limitation principles and the EU AI Act's prohibition of real-time biometrics in public spaces) creates dangerous jurisdictional arbitrage. Left unaddressed, these gaps threaten to normalize a digital panopticon where unaccountable surveillance: (a) chills democratic participation through self-censorship, (b) automates caste-communal profiling via historically skewed datasets, and (c) erodes procedural justice through unexplainable AI decisions. The analysis contends that only urgent statutory intervention—mandating algorithmic impact assessments, independent bias auditing, and judicial warrants for surveillance deployment—can reconcile technological efficacy with India's foundational rights architecture.

ISSN: 2582-6433

I. INTRODUCTION

"India's rapidly expanding deployment of artificial intelligence for public surveillance[1]—notably facial recognition systems, predictive policing algorithms, and mass data analytics—fundamentally challenges constitutional privacy protections. Despite the Supreme Court's landmark affirmation of privacy rights in Justice K.S. Puttaswamy v. Union of India (2017)[2], these technologies frequently operate without parliamentary authorization or judicial oversight[3], directly violating Puttaswamy's essential requirements of legality, necessity, and proportionality. The inherent opacity of 'black box' algorithms compounds these concerns by embedding systemic biases that disproportionately target marginalized communities[4], thereby undermining equality guarantees under Articles 14–15 within India's complex socio-legal landscape. This paper interrogates these tensions through dual frameworks: analyzing domestic jurisprudence on state accountability for technological overreach,[5] while evaluating India's regulatory alignment with emerging global standards like the GDPR's data protection principles[6] and the EU AI Act's risk-based classifications.[7] It argues that unconstrained surveillance automation risks institutionalizing extra-legal public monitoring—a digital panopticon[8] eroding democratic safeguards. Consequently, the study advocates urgent legislative intervention establishing algorithmic impact assessments, independent oversight bodies, and bias auditing mandates[9] to reconcile security objectives with fundamental rights."

II. ARTIFICIAL INTELLIGENCE AND PUBLIC SURVEILLANCE IN INDIA

The deployment of AI-powered public surveillance systems, such as National Automated Facial Recognition System (NAFRS)[10] in India, showcases the unchecked and unlawful collection, processing, and fiscal surveillance of sensitive biometric information[11], which greatly infringes upon the right to privacy as discussed in the Supreme Court case of Justice K.S. Puttaswamy (Retd) vs. Union of India (2017). These systems operate in a significant legal gap[12], devoid of a legal framework passed by Parliament which permits the collection of biometric information on individuals for the purpose of state surveillance, failing to fulfill the Puttaswamy judgment which mandates privacy intrusions must be “just, fair, and reasonable.” These intrusions must be grounded in law, necessary and proportionate to a lawful state interest such as the investigation of serious crimes and must include strong safeguards against abuse. The manner NAFRS unlawfully obtains facial images is in itself highly invasive: individuals’ facial images are captured and identified in public via a networked system of surveillance

ISSN: 2582-6433

cameras which track people without explicit and informed consent. This dragnet collection, justified by the vague and overly broad objective of "crime prevention," lacks essential principles of purpose limitation and data minimization, directly contradicting constitutional requirements. The inherent nature of biometric data – its uniqueness, immutability (unlike passwords, it cannot be changed if compromised), and profound sensitivity[13] as intrinsic biological identifiers[14] – exponentially amplifies the risks associated with this unregulated regime. Compounding the acquisition concerns is the unregulated storage paradigm: NAFRS aims to centralize biometric data in vast repositories, often linking facial templates to other personal information, creating attractive targets for cyberattacks and enabling unprecedented state profiling capabilities. The absence of mandated data retention periods and strict deletion protocols creates a high risk of indefinite storage, perpetuating the threat of misuse long after any initial justification expires. Furthermore, without enforceable, auditable security standards tailored to biometric sensitivity, these centralized databases face significant vulnerability risks, exacerbated by India's history of government data breaches[15]; a compromise involving immutable biometric data would inflict irreversible harm.[16] This unregulated ecosystem facilitates dangerous "function creep," where data collected nominally for crime detection is easily repurposed for mass surveillance, social profiling, caste or religious targeting, or monitoring political dissent and lawful assemblies without consent. The consequences are severe and multifaceted: pervasive, unaccountable surveillance chills the exercise of fundamental freedoms (speech, assembly, movement), particularly impacting marginalized communities and dissenters; the documented inaccuracies and biases inherent in facial recognition algorithms (especially against women, darker-skinned individuals[17], and ethnic minorities, as evidenced by studies like those from NIST[18] lead to discriminatory false positives, wrongful detentions, and the amplification of societal prejudice; and the potential for continuous tracking enables the creation of detailed movement and association profiles of entire populations[19], fundamentally undermining the presumption of innocence. The recent Digital Personal Data Protection Act (DPDPA)[20] 2023 fails to adequately address this crisis, offering broad exemptions for state security agencies and lacking specific, stringent provisions to regulate biometric surveillance or prevent mass collection. Consequently, there is an urgent, non-negotiable need for dedicated legislation that explicitly governs state use of biometric surveillance, mandating strict purpose limitation (confined to investigating specific, serious crimes), prior judicial or independent authorization for deployment, rigorous data minimization and retention limits, prohibition of mass real-time identification without warrants based on probable cause, algorithmic transparency and bias auditing, robust security standards with

ISSN: 2582-6433

independent oversight, and effective redressal mechanisms for citizens, ensuring strict adherence to the Puttaswamy proportionality test to prevent the normalization of a rights-violating surveillance architecture.

III. CONSTITUTIONAL FOUNDATIONS OF THE RIGHT TO PRIVACY

The Indian right to privacy, now clearly recognized as a basic right under Article 21 of the Constitution, did not come from a specific law or direct text. Instead, it was developed slowly through court decisions that showed privacy is a natural part of the "right to life and personal liberty. " This process started early, like in the case of Kharak Singh v. State of Uttar Pradesh (1963)[21], where the Supreme Court, while stopping midnight police visits, actually said privacy wasn't a separate right under Article 21. However, a minority opinion by Justice Subba Rao pointed out that privacy could be seen as part of the "liberty" in Article 21 and the "dignity of the individual" in the Constitution's Preamble. This confusion continued through the Emergency period with the judgment in ADM Jabalpur v. Shivkant Shukla (1976)[22], where civil liberties were suspended, highlighting how fragile rights can be without strong legal backing. A big change came in the case of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)[23], where a nine-judge bench clearly said privacy is a fundamental right. The court said privacy is an important part of human dignity, self-rule, and personal identity under Article 21, based on the core of freedom. The court also pointed out where privacy comes from in the Constitution:

- Article 21: Protects important personal decisions (like marriage and having children), bodily freedom, and control over personal information.
- Article 19: Freedom of speech, movement, and association includes the right to think independently.
- Article 14: Discrimination by the state violates the idea of equality.
- Preamble & Dignity: Privacy is essential to the "dignity of the individual," which is at the heart of India's constitutional values.

Puttaswamy also created a system for looking at privacy invasions.

Any government action must meet four conditions: (i) it must be legal, (ii) serve a real state need, (iii) be the least harmful way, and (iv) be fair in terms of the harm it causes versus the

ISSN: 2582-6433

benefit. The court also divided privacy into three areas: (1) physical (like bodily privacy), (2) decision-making (like making your own personal choices), and (3) information (like control over your data), each needing different protection. The court also rejected the idea that privacy only applies to rich people, saying it's important for everyone, especially those who are disadvantaged. Justice Chandrachud said privacy helps people resist government power and makes democracy stronger. But some of the other judges raised concerns: Justice Nariman warned that privacy claims shouldn't be used to oppose social reforms, like the decriminalization of homosexuality[24]. Justice Kaul suggested the need for a data protection law to stop digital monitoring.

Today, the Puttaswamy decision is a key part of Indian constitutional law, influencing decisions involving rights (like in Navtej Singh Johar, 2018) and data regulations. However, there's still debate about how to apply it, especially when balancing state surveillance with individual freedom. The true impact of this decision is how it changed the idea of liberty—not just as a tool to block the government, but as a way to ensure people can live freely in a world with constant surveillance.

IV. AI SURVEILLANCE AND THE PROPORTIONALITY TEST

He use of AI-based surveillance by Indian government agencies must meet the four-part proportionality test outlined in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)[25] to pass constitutional checks. However, current practices fail at every stage of this test, making them both legally and morally wrong.

A. Legality: The Legal Gap

One major issue is the lack of a specific law from Parliament allowing the use of biometric surveillance[26]. Although the Information Technology Act, 2000[27] has some rules about data security (Sections 43A and 72A), it does not cover how state agencies collect or process biometric data. The Digital Personal Data Protection Act (DPDPA)[28], 2023, which was recently passed, also leaves out state bodies from key rules when data is linked to national security or public order (Section 17(2)(a)). This means systems like the National Automated Facial Recognition System (NAFRS)[29] are run through executive orders or old laws like the Identification of Prisoners Act, 1920[30].

This breaks the standard that privacy invasions must have a clear, specific, and predictable legal basis.

ISSN: 2582-6433

B. Legitimate Aim: Beyond General Excuses

While public safety and national security are valid reasons for government action under Article 21, they must be used carefully. In practice, AI surveillance is often used for purposes that go far beyond what is needed: facial recognition systems initially meant for crime prevention are regularly used to monitor protests and political events. In Shreya Singhal v. Union of India (2015)[31], the Supreme Court canceled Section 66A of the IT Act because it was too vague, stressing that any restriction on rights must have a clear purpose. AI surveillance lacks this clarity.

C. Necessity and Suitability: The Effectiveness Problem

Surveillance tools must be both suitable (logically linked to their aim) and necessary (the least restrictive option). AI tools fail on both counts: studies show that facial recognition systems perform worse for darker-skinned women, with error rates up to 10 to 100 times higher than for lighter-skinned men. In India, these errors can lead to unfair targeting during policing. Reports show that targeted surveillance is more effective than mass AI screening. The requirement of using the least invasive method is ignored by India's widespread collection of biometric data.

D. Balancing and Procedural Safeguards: Systemic Failures

Proportionality means that any privacy loss should be justified by significant public benefit. This balance breaks down without proper oversight: unlike the EU's GDPR[32], India lacks independent watchdogs. The Data Protection Board proposed under the DPDPA doesn't have the power to check state surveillance. Citizens can't access facial recognition watchlists or challenge false matches, which violates privacy rights.

Research shows mass surveillance reduces political participation[33], with 74% of people in India avoiding protests due to facial recognition systems[34]

V. LACK OF TRANSPARENCY AND ALGORITHMIC DISCRIMINATION

The deployment of artificial intelligence in India's public surveillance infrastructure operates under profound opacity, creating systems that function as impenetrable 'black boxes' devoid of meaningful explainability or accountability[35]. This technical obscurity manifests in two constitutionally corrosive dimensions: the absence of public disclosure regarding system

ISSN: 2582-6433

functionality, data sources, and decision-making logic; and the embedding of historical societal biases into algorithmic outputs through unrepresentative or skewed training data[36]. Such deficiencies directly contravene constitutional guarantees under Article 14 (equality before law) and Article 15 (prohibition of discrimination) by enabling disproportionate targeting of marginalised communities, including religious minorities, Scheduled Castes/Tribes, and gender non-conforming individuals[37]. The fundamental rights crisis emerges from the state's failure to mandate algorithmic transparency or independent bias audits, thereby permitting automated decisions that perpetuate and amplify structural inequities under the veneer of technological neutrality[38].

Empirical evidence from global contexts demonstrates the severity of this risk. Studies by the U.S. National Institute of Standards and Technology (NIST) confirm that facial recognition algorithms exhibit dramatically higher error rates—ranging from 10 to 100 times more inaccuracies—for darker-skinned individuals, women, and elderly demographics[39] compared to lighter-skinned men. These disparities stem from training datasets overwhelmingly composed of Caucasian male facial images, institutionalising racial and gender bias at the computational level[40]. In India, where caste and religious identities intersect with phenotypical characteristics, analogous risks manifest with heightened severity[41]. For instance, facial recognition systems trained primarily on urban, upper-caste populations may systematically misidentify rural Dalit or Adivasi communities, potentially triggering false criminal flags during policing operations[42]. Without legally enforced diversity standards in training data—as proposed by the Algorithmic Accountability Act frameworks in the EU and U.S.—these tools encode discrimination into public security infrastructure[43].

The constitutional violation is further compounded by India's regulatory vacuum. Unlike jurisdictions such as France (where the Loi Informatique et Libertés mandates algorithmic impact assessments)[44] or Canada (requiring bias mitigation reports under the Directive on Automated Decision-Making),[45] India possesses no legal requirement for transparency documentation, third-party algorithm validation, or public disclosure of accuracy metrics[46]. Consequently, systems like the National Automated Facial Recognition System (NAFRS) operate without published accuracy rates for diverse demographic groups[47], despite their deployment in policing and identity verification. This violates the Puttaswamy proportionality standard's procedural prong[48], which necessitates oversight mechanisms to prevent arbitrary state action. Moreover, the discriminatory outcomes contravene Supreme Court jurisprudence

ISSN: 2582-6433

affirming that state use of technology must not violate substantive equality (Navtej Singh Johar, 2018). When facial recognition misidentifies a Muslim individual at a protest site or falsely flags a transgender person due to dataset gaps, it operationalises algorithmic violence that reinforces existing social hierarchies—effectively digitalising casteist or communal prejudice through state machinery[49].

Addressing this crisis requires urgent legislative intervention mandating: (1) public algorithmic registries disclosing training data sources and performance metrics; (2) compulsory bias audits by accredited independent entities; (3) redress mechanisms for affected individuals; and (4) prohibition of high-risk AI applications until equity thresholds are met. Absent these safeguards, India's AI surveillance architecture risks formalising unconstitutional discrimination under the false pretence of technological progress.

VI. CASE STUDIES FROM INDIA: DELHI, HYDERABAD AND BEYOND

The operational deployment of artificial intelligence-driven surveillance systems across Indian cities reveals a pattern of constitutional disregard, with Delhi and Hyderabad serving as emblematic case studies. During the anti-Citizenship Amendment Act (CAA) protests in Delhi[50] law enforcement agencies extensively utilized facial recognition technology (FRT) for mass crowd monitoring and identification of demonstrators. This deployment occurred without prior judicial authorisation[51], public disclosure of accuracy metrics[52], or adherence to purpose limitation principles. Cameras installed at protest sites and entry points captured biometric data en masse, cross-referencing live feeds against criminal databases and undefined "suspect" watchlists[53]. The absence of operational guidelines allowed for arbitrary identification of individuals engaged in peaceful assembly[54], directly infringing upon the right to dissent protected under Article 19(1)(a) of the Constitution. At the same time, the Hyderabad Police initiated one of India's most advanced surveillance systems through its "T Suraksha Command and Operations Public" program. The system comprised mobile surveillance vans armed with automatic license plate reader technology and body cameras, in addition to handheld facial-recognition devices carried by police in the guise of "smart glasses." Such devices facilitated real-time biometric identification of pedestrians and motorists during routine patrols, absent warrants or clearly articulated procedures. Particularly noteworthy were applications in majority-Muslim areas like Charminar and public events, where algorithmic identification was

ISSN: 2582-6433

carried out without consent or reasonable suspicion. These technologies effectively converted routine public movement into continuous identity verification processes, thereby rendering suspicionless surveillance the new norm in contravention of the Puttaswamy proportionality standard.

Outside these cities, the same trends are widespread in at least 16 Indian states under Central Government initiatives such as the Safe City Mission and Integrated Smart Control Centre programs. Punjab utilizes FRT-enabled drones tracking farm protest locations, and Chennai uses emotion recognition software at transport hubs with "pre-crime" detection assertions. Serial constitutional abuses are widespread: absence of legislative sanction allowing function creep (where "crime prevention" tools target minorities and activists), lack of mandatory accuracy audits despite reported racial profiling, and inaction to provide redress mechanisms for erroneous identifications. Psychological effects are dire – surveys show over 68% of surveilled area respondents self-censor online speech and steer clear of public gatherings. Such effects effectively alter the character of public space from expressive freedom spaces to spaces of state-mediated control of behavior. Critically, such deployments occur without satisfying the four-tantamount Puttaswamy test: they are not legal (no parliamentary legislation allows dragnet biometric collection), offend proportionality of legitimate aim (targeting constitutionally protected activities such as protests), ignore necessity (using highly error-prone devices where conventional policing is adequate), and ignore procedural safeguards (no independent oversight or consent requirements). Such normalization of extra-constitutional surveillance sets a perilous precedent where technological feasibility supplants fundamental rights, allowing profiling with disproportionate effect against religious minorities, Dalit communities, and political dissidents under the camouflage of algorithmic objectivity.

VII. COMPARATIVE LEGAL FRAMEWORKS

A. European Union: Rights-Based Technological Governance

The European Union sets the global standard for rights-respecting AI governance with its cohesive system of the General Data Protection Regulation (GDPR) and innovative Artificial Intelligence Act. GDPR enshrines foundation principles such as data minimization (limiting data collection to only the absolutely necessary data), purpose limitation (excluding secondary use without clear consent), and express opt-in consent for processing biometric data, establishing enforceable individual rights to access, correct, and erase personal data. On this foundation, the innovative AI Act takes a risk-based categorization approach that deems real-

ISSN: 2582-6433

time public facial recognition as "high-risk," subjecting it to strict requirements: mandatory fundamental rights impact assessments, algorithmic transparency notices, and ongoing human oversight requirements. Most importantly, the system bars predictive policing systems and emotion recognition in law enforcement, establishing ethical limits lacking in most Global South regimes. This model illustrates how technological efficacy can be combined with constitutional protection via ex-ante regulatory stringency.

B. United States: Decentralized Enforcement and Aspirational Standards

Unlike Europe's across-the-board approach, the United States implements its sectoral strategy pursuant to the Federal Trade Commission's (FTC) consumer protection mandate[55] instead of omnibus privacy legislation. The FTC enforces algorithmic accountability under Section 5 of the FTC Act by bringing suit against companies for "unfair or deceptive practices" in discriminatory AI system cases against consumers, such as against Clearview AI[56] for non-consensual face scraping. Without statutory biometric protections, the White House's 2022 Blueprint for an AI Bill of Rights[57] articulates necessary non-binding principles: robust pre-deployment testing for algorithmic bias, opt-out for automated systems, and transparency requirements for government AI deployments. Leading states have enacted these standards; Illinois' Biometric Information Privacy Act (BIPA)[58] requires consent for biometric collection and includes a private right of action, and it has produced landmark settlements against tech companies violating facial recognition ethics. This patchwork regime strikes a balance between innovation and emergent protection of rights through litigation-driven accountability.

C. China: Authoritarian Surveillance as State Policy

China offers a diametrically opposite model where AI surveillance is an apparatus of state control rather than rights preservation. No data protection legislation or judicial oversight enables mass deployment of integrated surveillance systems – combining facial recognition cameras, gait analysis, and predictive algorithms on 600 million CCTV endpoints. Xinjiang is the model for this system: Uyghur minorities are forced to undergo mandatory DNA and biometric extraction, with AI systems cross-matching mobility patterns, social relationships, and even emotional micro-expressions to activate "pre-crime" detentions in re-education camps. The 2020 Social Credit System materializes algorithmic discrimination by limiting travel, education, and employment based on opaque behavioural scoring. China's legal system actively enables this by requiring corporate data-sharing with security agencies under the 2017 National Intelligence Law[59] and 2021 Personal Information Protection Law's[60] sweeping

ISSN: 2582-6433

"national security" exceptions. This illustrates how untrammeled surveillance technology deconstructs privacy and equality when subjected to authoritarian control.

Synthesis: Varied Philosophical Approaches, Converging Issues

These models reveal underlying philosophical fault lines: the EU prioritizes human dignity through anticipatory checks on state-corporate power; the US has recourse to ex-post solutions and market standards; China employs technology as an instrument of social control. All three jurisdictions, nonetheless, share similar challenges of regulating rapidly emerging generative AI and deepfake technologies. Most urgently, India's regulation trajectory currently follows China's operational scale without even China's nominal statutory regimes – as a cautionary example where technological adoption outruns constitutional protection. The comparative analysis underlines that effective protection of rights requires more than technical compliance but interspersed democratic oversight mechanisms that are absent in India's surveillance architecture.

VIII. RECOMMENDATIONS FOR A REGULATORY FRAMEWORK IN INDIA

To balance AI surveillance with constitutional protection, India needs toimplement a rights-based regulatory framework through near-term tripartite reforms. First, sweeping legislative action needs to amplify the Digital Personal Data Protection Act (DPDPA), 2023 by: (i) removingblanket exceptions to state surveillance under Section 17(2)(a); (ii) clearly regulating processing of biometric data under a separatestatutory chapter; and (iii) making Privacy Impact Assessments (PIAs) mandatory for all surveillance projects with documented proportionality, necessity, and discrimination risk assessment beforedeployment. Second, institutional accountability necessitates creating a statutory Data Protection Authority (DPA)[61] vested with powers to: (a) conduct independent audits of AI systems[62]; (b) investigate public complaints regarding surveillance misuse[63]; and (c) enforce prior authorisation protocols where surveillance deployment requires approval from judicial or specialised quasi-judicial bodies[64], mirroring the EU's 'prior consultation' model under Article 36 of the GDPR[65]. Third, algorithmic transparency must be operationalised by obligating public agencies to: (1) disclose training datasets, accuracy metrics, and decision-making logic in public registries[66]; (2) subject systems to mandatory quarterly bias testing by accredited third parties using NIST-type demographic variance benchmarks[67]; and (3) implement real-time explainability

ISSN: 2582-6433

mechanisms[68] enabling affected individuals to understand automated decisions. Crucially, this framework must criminalise function creep[69] by prohibiting repurposing of surveillance data beyond legislatively specified purposes and establish accessible redress channels—including algorithmic compensation tribunals—for victims of misidentification or profiling[70]. Only through such multilayered governance, anchoring technological deployment to the Puttaswamy proportionality standard[71], can India prevent state surveillance from eroding its constitutional democracy.

IX. CONCLUSION

AI-driven surveillance represents an unprecedented threat to India's constitutional architecture, systematically eroding the fundamental right to privacy affirmed in Puttaswamy through technologically enabled state overreach. The absence of dedicated legislation governing biometric data collection, coupled with opaque algorithmic systems exhibiting documented racial and caste-based biases, institutionalises discrimination against marginalised communities while enabling mass surveillance devoid of proportionality or necessity. Function creep—where tools deployed for "public safety" target protesters and minorities—and the chilling effect on democratic participation reveal the incompatibility of unregulated AI with Articles 14, 15, and 19. Current frameworks, including the DPDPA's exemptions for state agencies, fail constitutional muster under the Puttaswamy test by lacking legality, legitimate aim specificity, and procedural safeguards. To prevent the normalization of a digital panopticon, India must urgently enact surveillance-specific legislation mandating judicial warrants for AI deployment, independent bias audits, algorithmic transparency registers, and robust redress mechanisms. Technological progress must not eclipse constitutional accountability; only through embedding AI governance within India's rights-based framework—ensuring technology serves liberty rather than subverts it—can democratic equilibrium be preserved.

[1] Amnesty International, *India: Facial Recognition Systems Must Be Banned* (2021).
[2] *Justice KS Puttaswamy (Retd) v. Union of India* (2017) 10 SCC 1.
[3] SFLC.in, *Legal Vacuum in Policing Tech* (2023)
[4] Centre for Internet & Society, *AI & Caste Discrimination* (2023).
[5] *People's Union for Civil Liberties v. Union of India* (1997) 1 SCC 301.
[6] Regulation (EU) 2016/679 (GDPR).
[7] European Parliament, *Artificial Intelligence Act* (2024).
[8] S. Annavarapu, 'Caste in the Machine' (2021) 55 *Sociological Bulletin* 112.
[9] High-Level Expert Group on AI (EU), *Ethics Guidelines* (2019).

ISSN: 2582-6433

[10] National Crime Records Bureau, *RFP for NAFRS* (2019).
[11] ISO/IEC 24745:2022 *Biometric Information Protection*.
[12] *Aadhaar Judgment* (2019) 10 SCC 1 [332] (Chandrachud J).
[13] Buolamwini J and Gebru T, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research 1.
[14] ISO/IEC 24745:2022 *Information Security, Cybersecurity and Privacy Protection — Biometric Information Protection*.
[15] The Tribune, *Aadhaar Data Breach Report* (4 January 2018)
[16] Reidenberg JR, 'Function Creep in Surveillance Systems' (2015) 37 *Cardozo L Rev* 101
[17] ISO/IEC 24745:2022 *Information Security, Cybersecurity and Privacy Protection — Biometric Information Protection*.
[18] Digital Personal Data Protection Act 2023 (India).
[19] Kishan V and others, *Moving from Legality to Legitimacy: The Case for Regulating Facial Recognition Technology in India* (CCG-NLUD 2023).
[20] Digital Personal Data Protection Act 2023 (India).
[21] *Kharak Singh v. State of UP* AIR 1963 SC 1295
[22] *ADM Jabalpur v. Shivkant Shukla* (1976) 2 SCC 521.
[23] *Justice KS Puttaswamy (Retd) v. Union of India* (2017) 10 SCC 1.
[24] *Navtej Singh Johar v. Union of India* (2018) 10 SCC 1.
[25] *Justice KS Puttaswamy (Retd) v. Union of India* (2017) 10 SCC 1.
[26] Shreya Singhal v. Union of India (2015) 5 SCC 1.
[27]Information Technology Act 2000 (India).
[28] Digital Personal Data Protection Act 2023 (India).
[29] National Crime Records Bureau, *Request for Proposal for National Automated Facial Recognition System (AFRS)* (NCRB 2019).
[30] Identification of Prisoners Act 1920 (India). [31] *Shreya Singhal* ().
[32] Regulation (EU) 2016/679 (General Data Protection Regulation).
[33] Penney JW, 'Chilling Effects: Online Surveillance and Wikipedia Use' (2016) 31 Berkeley Tech LJ 117.
[34] Software Freedom Law Centre India, *Citizen Survey on Facial Recognition Technology in India* (SFLC.in 2023).
[35] S. Annavarapu, 'Caste in the Machine' (2021) 55(2) *Sociological Bulletin* 112.
[36] M. Eubanks, *Automating Inequality* (St. Martin's Press 2018) 87.
[37] Centre for Internet & Society (CIS), *AI & Caste Discrimination in India* (Report, 2022) 15.
[38] S. Barocas and A. Selbst, 'Big Data's Disparate Impact' (2016) 104 *California Law Review* 671.
[39] P. Grother et al, *Face Recognition Vendor Test Part 3: Demographic Effects* (NISTIR 8280, 2019) 15.
[40] J. Buolamwini and T. Gebru, 'Gender Shades' (2018) *Proc. Machine Learning Research* 81, 77.
[41] A. Narayanan, 'Translation Tutorial: 21 Fairness Definitions' (2018) *ACM FAccT Conference* 2.
[42] N. Sambasivan et al, '"Everyone Wants to Do the Model Work"' (2021) *CHI '21* 1, 12. [43]European Commission, *Proposal for an Artificial Intelligence Act* (COM/2021/206 final) Art 10. [44]Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [France], Art 22.
[45] Treasury Board of Canada, *Directive on Automated Decision-Making* (2020) s 6.1.
[46] *Navtej Singh Johar v. Union of India* (2018) 10 SCC 1.
[47] National Crime Records Bureau, *RFP for NAFRS* (2019) Annexure IV.
[48] *Justice KS Puttaswamy (Retd) v. Union of India* (2017) 10 SCC 1 [148].
[49] Amnesty International, *Automated Harassment* (2022) 22.
[50] Amnesty International, *India: Facial Recognition Systems Must Be Banned in Protest Crackdown* (2021) 8
[51] Software Freedom Law Centre India (SFLC.in), *FRT Deployment in Delhi Protests* (2020) 12.
[52] Internet Freedom Foundation (IFF), *Unchecked Power: FRT at Protests* (2021) 5.
[53] SFLC.in, *Delhi Police FRT Watchlists* (2020) 9.
[54] *Shreya Singhal v. Union of India* (2015) 5 SCC 1.
[55] Federal Trade Commission Act 1914 (US).
[56] *In re: Clearview AI FTC Complaint* (2022).

ISSN: 2582-6433

[57] White House, *Blueprint for an AI Bill of Rights* (2022).
[58] Biometric Information Privacy Act 2008 (Illinois).
[59] National Intelligence Law of China (2017).
[60] Personal Information Protection Law of China (2021).
[61] Justice B.N. Srikrishna Committee, *Report on Data Protection Framework* (MeitY 2018) Rec.
[62] Algorithmic Accountability Act of 2022 (US) s 4(b).
[63] Regulation (EU) 2016/679 (GDPR) Art 57(1)(f).
[64] Justice KS Puttaswamy (Retd) v. Union of India (2017) 10 SCC 1 [487].
[65] GDPR Art 36.
[66] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique [France] Art 4.
[67] Grother P et al, Face Recognition Vendor Test Part 3: Demographic Effects (NISTIR 8280, 2019) 20-22.
[68] High-Level Expert Group on AI (EU), *Ethics Guidelines for Trustworthy AI* (2019) 16.
[69] Reidenberg JR, 'Function Creep in Surveillance Systems' (2015) 37 Cardozo L Rev 101, 112.
[70] European Commission, Proposal for an AI Liability Directive (COM/2022/496) Art 3.
[71] Puttaswamy (n 52) [159].