INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

SURVEILLANCE THROUGH AI AND RIGHT TO PRIVACY UNDER ARTICLE 21

AUTHORED BY - SHOBHIT MALIK

Introduction

The convergence of artificial intelligence (AI) and state surveillance has produced a profound crisis of constitutional law, a transmutation of the balance of sovereign power and individual liberty. Today, in the age of technology, the State has transcended physical surveillance, creating what Michel Foucault, drawing on Jeremy Bentham, called a "panopticon," but now undoubtedly digital, algorithmic, and exponentially more pervasive.[1]

The "Digital Panopticon" doesn't work with the visible gaze of a prison guard but with the invisible and continuous, pre-emptive collection of biometric data, metadata and behavioural patterns. Consider Artificial Intelligence processes like Automated Facial Recognition Systems (AFRS) or predictive policing algorithms. They do not merely record reality, but they probabilistically analyze, categorize and predict human behavior. This creates a pervasive chilling effect on civil liberties as the citizen is made permanently visible to the State, while the State's algorithmic architecture is shrouded in "black-box" opacity[2]. In order to understand the constitutional tension born out of this asymmetry, one must first follow the evolutionary arc of Article 21 of the Constitution of India, which has transformed from a sterile textual guarantee to the living repository of human dignity.

During the first years of the Republic, the Supreme Court took a very pedantic and restrictive view of Article 21[3]. In A.K. Gopalan v. State of Madras[4], the Court amputated Article 21 from Article 19[5], reading them in mutually exclusive silos. The majority interpreted "procedure

[1] Michel Foucault, Discipline and Punish: The Birth of the Prison 200 (Alan Sheridan trans., Vintage Books 1977) (1975).
[2] Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power 285–300 (2019) (describing the shift from monitoring to "actuating" behavior through predictive modeling); see also Oscar H. Gandy, Jr., The Panoptic Sort: A Political Economy of Personal Information 15 (1993) (discussing the discriminatory categorization of citizens).
[3] Const. India art. 21. Protection of life and personal liberty. No person shall be deprived of his life or personal liberty except according to procedure established by law.
[4] A.K. Gopalan v. State of Madras, A.I.R. 1950 S. C. 27
[5] Const. India art. 19. Protection of certain rights regarding freedom of speech, etc.

ISSN: 2582-6433

established by law" to mean only a law validly passed by the State and explicitly rejected the American doctrine of "due process". Under the Gopalan paradigm, substantive fairness/unreasonableness of a law was immune from judicial review. If this limiting textualism had stood the test of time, the contemporary digital surveillance regime could have simply been legalized by the passing of a draconian statute, and the citizen would have been left entirely defenseless against arbitrary algorithmic profiling.

However, the jurisprudential tectonic plates shifted dramatically with Maneka Gandhi v. Union of India.[6] In Maneka, the Supreme Court dismantled the Gopalan silos, finding an organic nexus between Articles 14[7], 19 and 21, the "Golden Triangle" of the Constitution. The Court held that "procedure established by law" cannot be arbitrary, fanciful or oppressive but must satisfy the test of being "right, just and fair." This meant the sub silentio importation of substantive due process into Indian constitutional law. The Maneka Gandhi ruling effectively made it mandatory that any state action which deprives an individual of personal liberty must be substantively reasonable, which implicitly includes informational autonomy and spatial privacy.

This evolution is relevant to our analysis of AI surveillance. The expansive reading of Article 21 in Maneka laid the normative foundation for pushing back against the modern surveillance state. It was held that state action cannot be saved from judicial review on the ground that it is supported by a statute, it has also to pass the test of fairness and non-arbitrariness. The primary constitutional bulwark as the State deploys AI-driven mass surveillance networks is the substantive due process architecture that emerged in Maneka. The argument is that algorithmic surveillance regimes need to be empirically justified, narrowly tailored and procedurally robust.

Privacy: Its Constitutional Underpinnings

The jurisprudential seeds sown in Maneka Gandhi were fully borne out in the landmark ruling of the nine-judge bench in Justice K.S. Puttaswamy (Retd.) v. Union of India.[8] Overruling the regressive dicta in M.P. Sharma[9] and Kharak Singh[10] denied privacy as a fundamental right,

[6] Maneka Gandhi v. Union of India, (1978) 1 S.C.C. 248 (India).
[7] Const. India art. 14. Equality before law.
[8] Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[9] MP. Sharma v. Satish Chandra, A.I.R. 1954 S. C. 300 (India) .
[10] Kharak Singh v. State of U.P., A.I.R. 1963 S.C. 1295 (India).

ISSN: 2582-6433

unequivocally anchored the right to privacy in the bedrock of dignity and autonomy under Article 21. Puttaswamy is not only declaratory. It provides a rigorous normative framework for the evaluation of the legitimacy of state intrusions. The Court recognized that privacy is multi-dimensional including spatial, decisional and informational privacy. AI surveillance is a fundamentally catastrophic violation of informational privacy, wherein the human subject is at all times a traceable data point.

Puttaswamy established a demanding, three-part proportionality test (sometimes conceptualized as including a fourth part of procedural safeguards) that any privacy-invading measure must pass, in order to restrain state power and avoid the loss of individual liberty under the guise of security. Assessed in light of these pillars – Legality, Legitimate State Aim (Need) and Proportionality. State's use of AI-based surveillance systems suffers from grave constitutional infirmities.

1. Lex (Pillar of Legality)

The first prong is that any privacy restriction has to be based on a passed law. Constitutional invalidity of executive fiats, departmental circulars or internal police directives. The law must be clear, accessible and foreseeable and define the precise conditions under which surveillance may be authorized.

At present, the use of AI surveillance in India, including municipal facial recognition grids or drone-based policing, is often in a statutory vacuum, relying on broad administrative orders rather than specific parliamentary enactments. Section 69 of the Information Technology Act, 2000[11] provides the authority for interception, monitoring and decryption of digital information, but was conceived for targeted surveillance of specific digital communications and not for mass, indiscriminate, algorithmic scraping of public spaces. Likewise, the recently enacted Digital Personal Data Protection (DPDP) Act, 2023,[12] while establishing a data protection framework, grants the State broad exemptions under Section 17(2)(a) for "interests of sovereignty and integrity of India, security of the State, [and] maintenance of public order." Yet, an exemption from data protection obligations alone is not equivalent to a substantive, enabling law that explicitly authorizes and regulates AI surveillance. Much of the state's current AI deployment is constitutionally ultra vires under the first prong of Puttaswamy, given the absence of a particular algorithmic surveillance law.

[11] Information Technology Act, 2000, Sec. 69, No. 21, Acts of the Parliament, 2000 (India).
[12] Digital Personal Data Protection Act, 2023, Section 17(2)(a), No. 22, Acts of Parliament, 2023 (India).

ISSN: 2582-6433

2. The Pillar of Legitimate State Purpose (Need)

The second prong requires that the State show a legitimate aim such as national security, counter-terrorism or prevention of serious crime. What is not in question is the legitimate state interest of maintaining public order. The requirement for AI surveillance must be empirically necessary and not be a product of speculative paranoia.

The State often invokes the doctrine of parens patriae and the need to preserve order to argue for the use of predictive policing and AFRS. But there's a troubling dissonance when it comes to analytical scrutiny of AI algorithms. Machine learning models learn from historical data that is inherently poisoned by systemic prejudices and institutional biases that target marginalized communities. In practice, the "need" expressed by the state often translates into the algorithmic profiling and over-policing of vulnerable socio-economic groups. The means adopted by a state to be constitutionally valid under Article 21 cannot be inherently discriminatory (violative of Article 14). If an AI surveillance system is, by design, generating false positives with racial or communal bias, then its use cannot be justified on the basis of a "legitimate aim".

3. The Proportionality Principle (Rational Nexus & Least Restrictive Means)

The third and most stringent prong is proportionality stricto sensu. The State must demonstrate that there is a rational connection between the AI surveillance used and the goal pursued and that it has used the "least restrictive means" to achieve that goal. This is where the constitutional test of AI-based surveillance fails most conspicuously.

Traditional surveillance, even as acknowledged in PUCL v. Union of India,[13] works on a model of targeted suspicion. Probable cause is the basis for issuing a warrant or authorization against a person. This paradigm is reversed in AI surveillance, especially mass FRS. It is based on a generalized suspicion model, where it actively scans, tracks and analyzes the biometric data of thousands of innocent citizens in order to find one suspect. It treats the whole population as presumed criminals.

This dragnet approach does not meet the "least restrictive means" test. The State should not use a technological sledgehammer when a scalpel is needed. Mass collection of biometric data creates permanent digital dossiers, chilling freedom of movement and assembly. Besides, Puttaswamy has called for strong procedural safeguards against abuse. AI surveillance systems don't have algorithmic transparency. This means a citizen cannot challenge an automated classification or obtain any meaningful remedial action if they are a false positive. Until the

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

ISSN: 2582-6433

State can demonstrate that its AI systems will be subject to independent algorithmic auditing, governed by strict principles of minimization, and used only as a last resort, such technologies are inherently disproportionate, and an unconstitutional invasion of the spatial and informational privacy guaranteed by Article 21.

Statutory and legal vacuum architecture of the DPDP Act, 2023

While Puttaswamy laid down the constitutional mandate for informational privacy, the legislative response giving effect to this mandate is the Digital Personal Data Protection (DPDP) Act, 2023. A careful reading of the DPDP Act however suggests that instead of imposing strict limits on state surveillance, the law systematically protects the State from data minimization and proportionality obligations. The Act's broadly drafted exemptions create a "legal vacuum," where AI-based surveillance can occur with little or no judicial or regulatory oversight.

However, section 7 of the DPDP Act deviates from strict consent architectures by allowing processing of personal data without explicit consent of the data principal for "certain legitimate uses". Section 7(b) is particularly disturbing considering the provision that the State or its instrumentalities can process personal data for the provision of any subsidy, benefit, service, certificate or license.[14]

In the context of AI and mass surveillance, it is easily weaponized. It provides a backdoor in the law for the State to amass huge volumes of biometric and demographic data under the benevolent cloak of welfare delivery. Section 7 effectively gives the State a limitless supply of non-consensual data, as algorithmic surveillance needs training data to enhance its predictive power. It legally disentangles the collection of citizen data from the requirement of informed consent, completely disregarding the informational self-determination espoused in Puttaswamy.

The most egregious departure from the proportionality standard is Section 17(2)(a) of the DPDP Act. The clause empowers the Central Government to exempt any instrumentality of the State from the operation of the provisions of the Act by notification in the interests of "sovereignty and integrity of India, security of the State, friendly relations with foreign States,

[14] Sec. 7(b). Digital Personal Data Protection Act, 2023

ISSN: 2582-6433

maintenance of public order or preventing incitement to any cognizable offence".[15]

Though these grounds are textually similar to reasonable restrictions under Article 19(2) of the Constitution, their application in the DPDP Act has no statutory requirement of necessity, proportionality or judicial oversight. The Act is not a regulatory mechanism because it permits the executive to unilaterally exclude its own law enforcement and intelligence agencies, the primary users of AI-based FRS and predictive policing, from data protection obligations. Rather, it creates a deliberate legal vacuum. In that vacuum, intelligence agencies have no purpose limitations, no data retention schedules, and no algorithmic transparency. Thus the DPDP Act, in contravention of the very purpose it claims to serve, provides a statutory shield for dragnet AI surveillance and does not satisfy the first and third prongs of the Puttaswamy test by not providing a clear, foreseeable law that guards citizens against arbitrary state intrusion.

The Mechanics of AI Surveillance

Understanding the unconstitutionality of AI surveillance requires more than abstract legal theory; it necessitates an examination of the practical mechanics of technologies like Automated Facial Recognition Systems (AFRS). The introduction of AFRS has specific phenomenological harms to civil liberties that are not present in traditional surveillance methods, including function creep, algorithmic bias, and the chilling effect.

The fallacy of the neutrality of AI algorithms, which are assumed to be mathematically objective, is dangerous. Machine learning models (for example, predictive policing, FRS etc.) are trained on historical criminal databases and policing records.[16] The history of policing in India is inextricably linked with systemic prejudices against marginalized communities – denotified tribes, religious minorities and lower-caste groups.

Training an algorithm on biased data doesn't eliminate bias, it institutionalizes and accelerates bias. This phenomenon is called "algorithmic bias." If an AFRS has a disproportionately high rate of false positives for minority demographics erroneously flagging innocent citizens as

[15] Id. at Sec. 17(2)(a).
[16] See Rashida Richardson et al., Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice, 94 N.Y.U. L. Rev. 192, 193–203 (2019) (discussing how historical police bias is encoded into algorithmic tools); see also Pamela Ugwudike, Algorithms, Policing, and Race, (2020) (critiquing the "myth of race neutrality" in predictive analytics).

ISSN: 2582-6433

suspects it is a clear violation of the guarantee of equality and equal protection under Article 14 of the Constitution. State action based on an algorithm biased on racial or communal lines is inherently arbitrary and renders the architecture of surveillance constitutionally void ab initio.

The architecture of AI surveillance is highly vulnerable to "function creep," the phenomenon of data collected for one specific, benign purpose being later used for a wholly different, unconsented and invasive purpose.[17]

In the Indian context, the State captures biometric data on a massive scale for welfare distribution (Aadhaar), vehicular regulation (Vahan), and pandemic management (CoWIN).[18] But without strict statutory purpose limitation, a gap the DPDP Act leaves wide open, these administrative databases regularly find their way into law enforcement FRS grids. When a citizen presents their photo to get a driver's license, they are not consenting to that image being scanned indefinitely by CCTV cameras at a political protest. Function creep turns civic administrative systems into latent punitive networks, dissolving the difference between the citizen as beneficiary and the citizen as suspect altogether.

The most insidious consequence of unrestrained AI surveillance is the "chilling effect" it has on core freedoms. In Anuradha Bhasin v. Union of India, the Supreme Court observed that state action that has a chilling effect on the freedom of speech and expression (Article 19(1)(a)) and freedom to assemble peaceably (Article 19(1)(b)) is constitutionally suspect.[19]

Citizens will very likely self-censor and refrain from exercising their democratic rights, knowing that their attendance at a protest, their gathering in public squares, or their association with political dissidents will be followed by real-time algorithmic biometric tracking. The chilling effect is implicit. The State does not need to explicitly prohibit a protest to stop citizens from going to it if the mere presence of AFRS stops them. Unregulated use of AI surveillance not only violates privacy (Article 21) but is also a structural assault on the democratic freedoms

[17] The Supreme Court has repeatedly warned against the perils of function creep and the necessity of purpose limitation in K.S. Puttaswamy v. Union of India, (2019) 1 S.C.C. 1 (India)
[18] See Reetika Khera, Dissent on Aadhaar: Big Data Meets Big Brother 12–35 (2019) (discussing the scaling of biometric data for welfare); see also Faiza Rahman, Digital Sovereignty and the Datafication of the Indian Citizen, 12 Indian J. Const. L. 45, 52–60 (2023) (analyzing the integration of Vahan and CoWIN into the state's surveillance architecture).
[19] Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India)

ISSN: 2582-6433

(Article 19) enshrined in the digital panopticon's silent, invisible architecture that stifles political dissent.

Judicial Precedents: From Physical Intrusions to Digital Wiretaps

The constitutional jurisprudence on state surveillance in India has been a tale of the tug-of-war between the executive's mandate to maintain public order and the judiciary's duty to protect individual autonomy. To gauge the scale of the threat that AI surveillance poses, one must juxtapose the landmark physical era judgments, especially Kharak Singh, with the strict procedural limitations that contemporary courts demand in matters such as Vinit Kumar.[20]

In Kharak Singh v. State of U.P.,[21] the Supreme Court had to consider the U.P. Chapter XX Police Regulations allowing "domiciliary visits" and secret picketing against history-sheeters.[22] Under the restrictive Gopalan framework, the majority struck down domiciliary visits but upheld secret picketing, ruling that the right to privacy was not guaranteed by the Constitution. Under Article 21 they equated personal liberty with freedom from physical restraint.

But the crux of the case, both in jurisprudential and intellectual terms, lies in the seminal dissent of Justice K. Subba Rao. Justice Subba Rao cleverly argued that privacy is an essential ingredient of personal liberty. Constant surveillance puts a 'psychological restraint' on the individual. He maintained that the citizen under constant surveillance, though free in body, is functionally imprisoned. His freedom of movement and thought is limited by the ever-watchful eye of the State.

Justice Subba Rao's concept of "psychological restraint" is the precise jurisprudential antecedent to the contemporary "chilling effect." Today, AI-based facial recognition is the digitized, infinitely scalable successor to the physical picketing depicted in Kharak Singh. A psychological enclosure is everywhere, algorithmically sorting citizens unseen. Puttaswamy explicitly elevated Justice Subba Rao's dissent to the level of binding constitutional law, holding that spatial and informational privacy are not peripheral rights but the very core of dignity under Article 21.

[20] Vinit Kumar v. Central Bureau of Investigation, 2019 SCC OnLine Bom 3155 (India)
[21] Kharak Singh v. State of U.P. A.I.R. 1963 S.C. 1295 (India) (J. Subba Rao, dissenting)
[22] U.P. Police Regulations, ch. XX, reg. 236 (India).

ISSN: 2582-6433

Strict Scrutiny by Vinit Kumar

J Subba Rao Having presented the theoretical framework, the modern operational strictures on surveillance were set down by the Bombay High Court in Vinit Kumar v. Central Bureau of Investigation.[23] In Vinit Kumar the State issued directions for interception of telephone messages against an individual suspected of economic offences. The State attempted to justify the surveillance under the cover of Section 5(2) of the Indian Telegraph Act, 1885[24], on the pretext of "public emergency" or "in the interest of public safety".

The Court held that the High Court was justified in quashing the interception orders and that economic offences do not amount to "public emergency" or "public safety". The Court reiterated the dictum in PUCL v. Union of India[25] that surveillance is a draconian measure and should be resorted to only as a last resort, when there is a demonstrable threat to a compelling and immediate state interest.

The legal gulf between the high procedural hurdles in Vinit Kumar and the present-day use of AI surveillance is staggering. To tap a single phone line, the State has to show a grave public emergency and follow strict rules of the review committee. By contrast, Automated Facial Recognition Systems scan, analyze and intercept the biometric "metadata" of millions of citizens in public spaces on a daily basis, in the absence of any independent warrants, review committees or demonstrated public emergencies. If the localized interception of one phone call requires rigorous judicial and procedural review, then the mass algorithmic interception of physical movements through AI cannot constitutionally survive without statutory underpinning.

Comparative Jurisprudence – The Case for a Risk-Based Taxonomy

A comparative jurisprudential analysis starkly exposes the inadequacies of the Indian framework. One major shortcoming of India's DPDP Act, 2023, is that it takes a monolithic, flat approach to data processing. It equates the collection of data for a simple e-commerce transaction with the deployment of complex, predictive law enforcement algorithms. In contrast, the European Union has decided that AI needs a completely new regulatory framework, leading to the Artificial Intelligence Act (Regulation (EU) 2024/1689).[26]

[23] Vinit Kumar v. Central Bureau of Investigation, 2019 SCC OnLine Bom 3155 (India)
[24] Indian Telegraph Act, 1885, Sec. 5(2).
[25] Supra Note 8
[26] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on harmonised

ISSN: 2582-6433

The EU AI Act: The 'Risk Based Approach'

The EU AI Act is a paradigm shift from classical data protection architectures by using a "Risk-Based Approach" that classifies AI systems into four categories – Unacceptable Risk, High Risk, Limited Risk, and Minimal Risk.

Notably, the Act explicitly categorizes "real-time" remote biometric identification systems deployed in publicly accessible areas for law enforcement purposes in the Unacceptable Risk category (Article 5), thereby virtually prohibiting them, with very narrow, judicially pre-authorized exceptions (e.g. targeted searches for victims of abduction or imminent terrorist threats). In addition, AI systems for biometric categorization, emotional recognition and predictive policing are firmly placed in High-Risk systems.

For High-Risk systems, the EU requires strict ex-ante (preventative) obligations. Such systems should be subject to rigorous fundamental rights impact assessments before deployment, include a "human-in-the-loop" oversight to avoid automated deprivations of liberty and ensure that training data is representative and free from systemic bias.

Why India Needs its Own AI Surveillance Taxonomy

The comparative analysis shows that India is trying to regulate 21st century algorithmic surveillance with 20th century paradigms. The broad exemptions under Section 17 of the DPDP Act conflict with the specific prohibitions put in place by the EU.

Urgency demands that a risk-based taxonomy be legislatively and judicially integrated with Indian jurisprudence so as to fill the constitutional void between state power and Article 21. AI surveillance is not just data processing. By definition, it is a "High-Risk" state activity which directly changes the relationship between sovereign and citizen. The three-pronged test of Puttaswamy inherently requires this: if an AI system poses a high risk to fundamental rights (because of algorithmic bias or dragnet capabilities), the procedural safeguards must be proportionately robust. The Supreme Court should require ex-ante Algorithmic Impact Assessments (AIA) and independent audits for any state agency that utilizes predictive or facial recognition technologies. The protections of Article 21 will be rendered meaningless by the vastness and obscurity of the State's digital panopticon, without the State adopting a risk-based

rules for artificial intelligence (Artificial Intelligence Act), 2024 O.J. (L 1689).

ISSN: 2582-6433

classification that legally recognizes the specific dangers of AI.

Theoretical Frameworks – Panopticism, Metadata and the Fear of Security

Constitutional law must engage with political philosophy in order to appreciate the full extent of the epistemic violence that state-led AI surveillance can cause. Critique of the statute is insufficient; we must interrogate the underlying mechanisms of power that the State employs to manufacture compliance.

In Discipline and Punish Michel Foucault noted how the power of the modern State is no longer exerted through spectacular acts of physical force (the public execution), but through the "disciplinary power" of continuous, silent, and meticulous observation of the individual.[27] The architectural embodiment of this is the Panopticon. The genius of panoptic power is that the citizen can never be sure at which precise moment he is being watched, and so he must internalize the gaze of the State and regulate his own behavior.

When Foucault theorized disciplinary power, he was concerned with the physical bodies locked away in prisons, schools, and hospitals. The State need not imprison the physical body any longer; it imprisons the citizen's "data double." Through the mass harvest of metadata, geolocation, communication frequencies, financial transactions, algorithmic facial recognition grids. The State creates a perfect digital replica of the individual. One could argue that metadata is even more revealing than the content of a communication itself, providing a glimpse into the entire architecture of a citizen's associations, predilections and political leanings.

This invisible algorithmic sorting is the most extreme disciplinary mechanism. This chilling of Article 21 and Article 19 freedoms is the perfect implementation of Foucault's panopticism: the citizen, aware of the metadata net but blind to the algorithms processing it, self-censors. The State achieves total psychological compliance without ever having to wave a physical baton.

This paradigm calls for a critical re-evaluation of the Social Contract. Thomas Hobbes and other classical theorists argued that individuals give up some of their natural liberty to the sovereign (Leviathan) in return for the security of life and property.[28] The modern surveillance

[27] Foucault, supra note 1, at 201-205.
[28] Thomas Hobbes, Leviathan 120-128 (Richard Tuck ed., Cambridge Univ. Press 1991) (1651).

ISSN: 2582-6433

state is heavily reliant on a Hobbesian justification: it asserts that the citizenry must cede its informational privacy (through the exemptions in the DPDP Act) in exchange for protection from terrorism, organised crime and public disorder.

But from the point of view of algorithmic fallibility, this transaction is a Faustian bargain that produces only a "mirage" of security. Predictive algorithms have been found to be rife with racial, caste and communal biases. AFRS systems are often inaccurate and can create many false positives. The citizen exchanges guaranteed, tangible constitutional freedoms (privacy, anonymity, speech) for a highly speculative, flawed and often biased promise of technological security.

Moreover, this deal violates the Lockean parameters of the Social Contract, which insists that the power of the sovereign must be strictly limited by the rule of law[29]. The State is trying to go beyond the legal limits of the contract by seeking broad exemptions under Section 17 of DPDP Act. The citizen is made completely transparent to the State and the State's algorithmic machinery is made completely opaque to the citizen. A fundamental breakdown of the constitutional reciprocity required in a democratic republic.

Conclusion

The conflict between AI surveillance and the right to privacy is the defining constitutional crisis of the twenty-first century. This treatise has demonstrated that the Indian State's move towards an algorithmic model of surveillance, with its mass data harvesting, automated facial recognition and predictive policing, is in effect a direct contravention of the golden triangle of Articles 14, 19 and 21. AI surveillance operates on a model of generalized suspicion that does not pass the strict proportionality test of Puttaswamy. At the same time, the legislative machinery built to protect the citizens, i.e., DPDP Act of 2023, has paradoxically created a legal vacuum that gives the State unrestricted exemptions that legitimize function creep and algorithmic bias.

The following specific structural policy interventions are urgently needed to save the Republic's constitutional soul from the invisible strictures of the digital panopticon:

1. Passage of a Standalone Surveillance and AI Regulation Act (SAIRA) The exemptions

[29] John Locke, Second Treatise of Government Para. 135 (1690)

ISSN: 2582-6433

under Section 17 of the DPDP Act should be struck down or severely circumscribed. "There should be a separate law on state surveillance passed by Parliament." It should clearly define the thresholds for the deployment of AI, in line with the EU AI Act's "Risk-Based Approach". It should define real-time, untargeted AFRS in public spaces as a "Unacceptable Risk" to be banned.

2. Creating a Judicial Oversight Commission of Surveillance: the present scheme of executive review (where the executive approves and reviews its own surveillance orders) is constitutionally at odds with the doctrine of separation of powers. An independent, permanent Judicial Oversight Commission comprising retired High Court or Supreme Court justices must be set up. No predictive policing algorithms or localized AFRS should be deployed without an ex-ante (prior) judicial warrant and issued only upon demonstration of a serious, immediate and proportionate threat to public safety.
3. Mandatory Algorithmic Impact Assessments (AIA): Any State instrumentality that deploys a machine-learning model for law enforcement must first undergo a mandatory independent Algorithmic Impact Assessment. Such an audit should look for systemic biases (caste, religion, gender) in the training data and also quantify the false-positive rates. If an algorithm fails the Article 14 neutrality test, then its use must be legally forbidden.
4. Statutory Protection of the Right to Algorithmic Transparency: A "Right to Explanation" should be the law for citizens when automated decisions impact their civil liberties. The "black-box" defense that law enforcement has been using must be invalidated statutorily. The State must be made to explain the logic parameters of any AI system that flags a citizen as a suspect.

The Constitution of India is an organic, living document, designed to survive not only the physical abuses of the 20th century, but the invisible algorithmic tyrannies of the future. The journey from Gopalan to Maneka and finally to Puttaswamy is a testament to the unflinching commitment of the Court to the broadening of the horizons of human dignity.

But if Article 21 has to survive the silicon age, the judiciary and legislature cannot afford to be technologically deferential any more. A constitution that can limit the physical truncheon of the police must be able to limit the source code of the State in the same way. This is the promise of personal liberty that will dangle in the suffocating web of the digital panopticon until the rule of law is hardwired into the architecture of artificial intelligence.