

**Swami Vivekananda Advanced Journal for Research and Studies**Online Copy of Document Available on: www.svajrs.com

ISSN:2584-105X

Pg. 451–462



Right to Privacy (Article 21) in the Age of AI: The Relevance of Fundamental Rights in the Era of Digital Surveillance, Data Processing, and Mass Profiling

Dr. Pravin Kumar Singh

Principal, S. M. Law College, Chandausi, Dist. Sambhal.

*Accepted: 12/06/2026**Published: 22/06/2026**DOI: <https://doi.org/10.5281/zenodo.23038136>*

Abstract

The evolution of Artificial Intelligence (AI) and large volume data has led to a post-digital world which will have a new outlook on human beings. Here everybody is under watch, and they have profiling. The Right to Privacy has been interpreted to be an integral part of Right to Life and Personal Liberty as guaranteed under Article 21 of the Indian Constitution. And with the dawn of digitalization, such a right is under constant threat from digital companies, the state, and others. The paper seeks to assess the efficacy of the fundamental rights in the changing scenarios of technological advancements, which have ultimately led to threats to the very privacy of individuals guaranteed under Article 21. By analysing the case study of K.S. Puttaswamy judgment, the Information Technology Act, 2000 and the Digital Personal Data Protection (DPDP) Act, 2023. The paper also tries to suggest a dynamic Constitutional framework which would create an algorithmic impact assessment to shield the citizens against unwanted digital surveillance and resultant discrimination on that basis.

Keywords: *Artificial Intelligence; Article 21; Right to Privacy; Puttaswamy Judgment; Digital Surveillance; Mass Profiling; Algorithmic Bias; Cyber Law; DPDP Act 2023.*

1. Introduction

The Indian Constitution is a living and growing document, which not only governs the people but also protects from the exploitation by the state. The basic structure of the constitution, which consists of Part III, Article 21 reads as "no person shall be deprived of his life or personal liberty except according to procedure established by law". Through active and progressive adjudication beginning with the *Maneka Gandhi v. Union of India* (1978),¹ Article 21 has, over decades, expanded to protect a plethora of rights that are integral to a dignified and prosperous society. However, the turn of the 21st century introduced a new factor, which the founding fathers of the constitution could not have possibly envisioned - the rise of Artificial Intelligence (AI) and the data economy it operates in.

Currently, the world finds itself in the middle of the Fourth Industrial Revolution, which is characterized by the convergence between the physical, digital and biological worlds.² In this data-centric paradigm, every interaction, transaction, association, and even geo-location of a person is transformed into data, which forms the lifeblood for AI. Modern AI is not like its rudimentary counterparts of the past, which only followed instructions. A lot of present-day AI systems use machine learning (ML) and neural networks for identifying patterns in data, which further allows them to make predictions and decisions.³

AFRS (Automated Facial Recognition Systems), predictive policing, welfare algorithms and other mass surveillance technologies have created a digital panopticon.⁴ The panopticon has taken a new turn in the algorithmic state with the power dynamics tilted heavily in favor of the state and the watchmen (private and public entities). A common citizen is always aware of being watched but is unable to know who is watching and when (or whether) they are being watched.⁵

AI is a serious threat to the newly recognized Right to Privacy in India. Though the Supreme Court of India in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017)⁶ has held that the Right to Privacy is a fundamental right, guaranteed under Article 21, the practical implementation of this right in an algorithmic state remains in question. The traditional torts of intrusion upon seclusion ("spatial privacy") and intrusion upon decisional privacy (protection of one's decision-making faculties) are no longer sufficient in the face of AI. This is because AI demands protection of informational privacy - a person's right to control

the collection, processing and dissemination of her information.

Furthermore, the threat is compounded by the phenomenon of "Surveillance Capitalism", a term coined by Shoshana Zuboff, where the human experience is converted into data, which is then exploited by private and state entities. Here, a public-private partnership is formed, where data obtained by private entities is shared with the state for enhancing surveillance capabilities. In such a scenario, mass surveillance using AI robs a person of their identity as the data subject is aggregated to create a statistical probability of that person's behavior and attitude, which is based on age-old prejudices.⁷

This paper attempts to evaluate whether Article 21 can effectively offer protection against such an existential threat. The paper argues that existing legal frameworks such as the Information Technology Act, 2000 and the new Digital Personal Data Protection (DPDP) Act, 2023 would be insufficient to tackle the "black-box" problem of AI. Thus, the paper recommends that the Indian Constitution must employ "Algorithmic Due Process" to protect the rights of the citizens.

2. The Indian Right to Privacy: Its Jurisprudential Origins and Development

Indian constitutional law's conception of the right to privacy has undergone a significant jurisprudential transformation over the course of more than 70 years. The Indian Constitution's framers did not specifically list the "Right to Privacy" as a separate fundamental right within Part III, in contrast to the United States Constitution, where the Fourth Amendment expressly protects citizens against "unreasonable searches and seizures," or the Universal Declaration of Human Rights (UDHR), which specifically mentions privacy under Article 12. The "living tree" theory of constitutional interpretation, in which the judiciary progressively broadened the definitions of "life" and "personal liberty" under Article 21 to address the changing complexity of contemporary society, is solely responsible for its inception.

2.1 Early Ambiguity: The Textualist Approach of the 1950s and 60s

In its early years, the Supreme Court of India took a very conservative and textual attitude toward the Constitution. The first major case concerning the privacy issue was *M.P. Sharma v. Satish Chandra* (1954)⁸. An eight-judge bench was tasked with

deciding the constitutionality of large-scale searches conducted by the police. The Court ruled that the right to privacy was not protected by the Constitution because it explicitly excluded it from its protection. The Court also stated that attempting to incorporate the American concept of the Fourth Amendment into the Indian Constitution would be fundamentally unconstitutional.

This narrow view was further tested but largely upheld in *Kharak Singh v. State of U.P.* (1962)⁹ which dealt with the constitutionality of police regulations allowing night visits and clandestine personal observation of 'history-sheeters'. The majority unequivocally declared that 'the right of privacy is not a guaranteed right under our Constitution'. However, the seeds for a more liberal approach were sown in the dissenting opinion of Justice K. Subba Rao who drew upon the American jurisprudence of Justice Felix Frankfurter. Justice Subba Rao contended that personal liberty in Article 21 is exhaustive. He held that constant surveillance creates a psychological fetter on the freedom of movement and that the sanctity of one's private space is intrinsic to the enjoyment of life.¹⁰

2.2 The Transitional Era: Penumbra Rights and Mental Privacy

As society evolved, the judiciary came to terms with the fact that a textual approach was too narrow, and the first step towards overcoming that problem was taken in *Gobind v. State of M.P.* (1975)¹¹. Inspired significantly by the American jurisprudence on 'penumbral rights' (*Griswold v. Connecticut*)¹², Justice K.K. Mathew held that the Right to Privacy was implicit in the penumbras of Articles 19(1)(a), 19(1)(d) and 21, but at the same time noted that this did not mean that this right was absolute and that it could be restricted by the state acting in the 'compelling state interest'.

This case by case, ad hoc recognition continued for decades. In *Malak Singh v. State of P&H* (1981)¹³, the Court held that while police could compile dossiers on citizens, surreptitious and intrusive investigations were prohibited as they were a violation of Article 21. Later, in *R. Rajagopal v. State of T.N.* (1994) (the *Auto Shankar case*)¹⁴, the Court explicitly formulated the tort of 'right to be let alone', which was linked to the right to privacy against the unauthorized disclosure of personal details.

A critical precursor to the AI and data processing debate was the case of *Selvi v. State of Karnataka*

(2010)¹⁵, which dealt with the constitutional validity of narcoanalysis and brain mapping. The Supreme Court acknowledged the concept of "Mental Privacy" and ruled that forcing an accused to disclose his or her inner self amounts to a violation of the right against self-incrimination (Article 20(3)) as well as substantive due process (under Article 21). In the era of AI, where algorithms attempt to profile psychological traits and predict behavior, the *Selvi* judgment serves as a crucial anchor against algorithmic cognitive intrusion.

2.3 The Aadhaar Catalyst and the Constitutional Crisis

The piecemeal approach to privacy left it extremely vulnerable to legal onslaughts. The vulnerability was on full display when the Union Government defended the Aadhaar project (world's largest biometric database) before the Supreme Court in the prolonged litigation. It is but this approach that led the Union Government to confidently argue before the Supreme Court that the privacy, although a common law right, is not protected as a fundamental right, citing the early judgments of *M.P. Sharma* and *Kharak Singh*.

This argument invited a massive constitutional crisis. If the state's position prevailed, it would have left the doors open to rampant state data mining, surveillance and biometric profiling of the people. A nine-judge Constitution Bench was convened to finally resolve the historic ambiguity and put the matter to rest.

2.4 The Watershed *Puttaswamy* Judgment: Privacy as an Inalienable Right

In a near-unanimous verdict in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017)¹⁶ the Supreme Court overruled the majoritarian view of privacy of fact that was espoused by *M.P. Sharma* and *Kharak Singh*. It declared that the Right to Privacy is an intrinsic part of the right to life and personal liberty under Article 21 and an essential ingredient of the freedoms guaranteed by Part III of the Constitution.

The plurality ruling by Justice D.Y. Chandrachud was especially important for the conversation around artificial intelligence and digital technologies. The ruling divided privacy into three separate but related aspects:

1. **Spatial Privacy:** Everyone has a right to spatial privacy, which refers to controlling one's physical space. The human body, home, property and other

private spaces must not be violated by the State or third parties without justification or warrant.

2. **Decisional Privacy:** Decisional privacy refers to the ability to make intimate and personal choices including those relating to sexual orientation, reproduction, family life and diet without interference, monitoring or scrutiny.
3. **Informational Privacy:** Privacy is the right of an individual to exercise meaningful control over the collection, processing, storage, use and dissemination of their personal information. In addition, to be protected from unauthorized disclosure or surveillance, and against unwarranted or harmful digitisation.¹⁷

The main constitutional defense against the algorithmic profiling, data scraping, and automated surveillance typical of the contemporary AI era is this third aspect, informational privacy.

2.5 The Proportionality Standard: A Constitutional Shield Against AI Overreach

Being fully cognizant that no fundamental rights inhere absolutely, the Puttaswamy bench laid down a very stringent four-part “proportionality” framework, largely inspired by the German Federal Constitutional Court’s and Supreme Court of Israel jurisprudence, that any law or state action invading privacy must undergo.¹⁸ Thus, for any state surveillance, say, using Automated Facial Recognition, predictive policing or data mining, to be found “justified” under Art 21, must pass the four-part test, namely:

1. **Legality (Procedure Established by Law):** For any interference by the State with the right to privacy, there must be a procedure established by law. Measures that involve AI-enabled surveillance cannot ordinarily be based only on executive notification or instructions or circulars issued by an authority.
2. **Legitimate State Aim:** Any restriction on the right to privacy must be in line with a legitimate interest of the State like national security, public order, prevention of crimes and efficient, equitable delivery of public goods and services.
3. **Suitability (Rational Nexus):** There must be a rational connection between the state's objective and the technological means adopted to achieve it.
4. **Necessity (Least Restrictive Measure):** In the perspective of AI, this is the most important prong. The state must demonstrate that the technology

used is the least restrictive way to accomplish the objective. Additionally, the invasion of rights must be carefully weighed against the benefits to society.

In the age of automated decision-making and mass surveillance, this very 'Proportionality Test' is the most powerful constitutional weapon. Whenever state agencies are going to apply 'black box' AI to make judgments over huge amounts of data, these are inherently systems which presume everyone is guilty until proven otherwise and hence are inherently 'least restrictive measures' and are thus outright forbidden by Article 21.

3. Digital Surveillance: The State's AI Panopticon

The state and surveillance: how have they changed throughout history? State interception used to be a targeted and physical process, where an agent would follow or listen in on a particular person of interest. With the help of new technologies such as Artificial Intelligence and Big Data, the practice has become much more automated and integrated into every day life. As surveillance becomes much more accessible, it threatens to tip the scales of the balance between state and liberty upheld by article 21.

3.1 The Shift from Targeted Interception to Mass Algorithmic Surveillance

The Indian laws that regulate surveillance are the Section 5(2) of the Indian Telegraph Act, 1885 and the Section 69 of the Information Technology Act, 2000. These laws were designed for a time when interception of communication was required on a targeted basis, and authorized the government to do so, in case of a public emergency or in the interest of public safety.¹⁹

However, the AI does not filter; instead, it collects and calculates. The state apparatus employs complicated machine learning algorithms to scan the social media of citizens, analyze their financial transactions, and process their location data. In such a scenario, there is no distinction between “targeted” and “mass” surveillance, and the authorities process the entire population to spot statistically significant suspicious activity or predict future crimes. This practice does not adhere to the principle of innocence until proven guilty, which is an integral part of criminal procedure and substantial due process rights under Article 21.²⁰

3.2 Automated Facial Recognition Systems (AFRS) and the CCTNS

In India, Automated Facial Recognition Systems are being adopted the fastest form of AI surveillance. An instance of this is the implementation by NCRB for the integration of a National Automated Facial Recognition System (NAFRS) with the Crime and Criminal Tracking Network & Systems (CCTNS). The latter refers to one of the digitised databases connecting police stations across the country which stores FIRs, charge sheets, and pictures of suspects.²¹

Parliamentary legislation should govern face recognition so that the surveillance does not occur in a legal vacuum. These deployments are inherently illegal as executive notice or administrative instructions are completely insufficient to satisfy the requirement of "procedure established by law" in Article 21.

3.3 The Constitutional Vulnerability: Failing the Proportionality Test

The state's vast AI surveillance apparatus always fails the strict four-pronged Proportionality Test set forth in Puttaswamy.

First, as mentioned, there is a serious lack of legality; there is no clear statutory support for widespread algorithmic surveillance. Second, although upholding public order is a legitimate state goal, indiscriminate surveillance does not meet the requirements of need and suitability.

The "least restrictive measure" doctrine demands that the state prove that mass surveillance is the only way to accomplish its goal, but dragging the whole society into the net to catch a few criminals is demonstrably disproportionate. Just as the Supreme Court held in the case of Aadhaar, the state cannot use a sledgehammer to crack a nut. Moreover, AI facial recognition is demonstrably inaccurate, and not only does it wrongly flag minority ethnicities and women, but it also results in false positives and detentions. Thus, employing an unreliable algorithm to deprive a citizen of his or her liberty is a manifestly unfair, unjust, and unreasonable procedure, a violation of the "fair, just, and reasonable" standard articulated by the Supreme Court in the Maneka Gandhi case.²²

3.4 The Chilling Effect on Democratic Freedoms

The harm caused by AI surveillance goes beyond the violation of privacy. It inflicts a chilling effect on the exercise of other fundamental rights such as the

rights of free speech and expression (Article 19(1)(a)) and the right to assemble peaceably (Article 19(1)(b)).

When citizens know that their presence at a protest, their digital communications or association with political dissenters are being recorded, categorized and stored in state databases (such as CCTNS) through AI, it leads to self-censorship.²³ The Supreme Court, in *Anuradha Bhasin v. Union of India* (2020)²⁴ held that the chilling effect on expression caused by state actions in digital sphere could violate constitutional rights. In the algorithmic state, the Right to Privacy acts as the precondition for realization of all other civil liberties. Without an absolute guarantee of the absence of mass digital surveillance, the democratic fabric woven by Part III of the Constitution stands to be unraveled by lines of code.

4. Mass Profiling, Data Processing, and Algorithmic Bias: The Erosion of Article 14

While digital surveillance focuses on collecting information about individuals, mass profiling concentrates on processing the data about the citizens by Artificial Intelligence (AI). The real issue with AI is that it can sort, rank, rate, and predict human lives at a scale that has never happened before. The state and capitalistic organizations that use such methods for making decisions about people's lives are distorting the equality and justice principle, which the Indian Constitution's Article 14 mandates to protect and safeguards.

4.1 The "Black Box" Problem and the Subversion of Substantive Due Process

The fundamental requirement of the "rule of law" (which is the basic structure of the Constitution) is transparency, accountability, and the ability for a citizen to challenge an adverse state action. However, the architecture of modern AI, particularly the deep learning neural networks, is a "Black Box."

These systems take in huge amounts of information, and then make judgments about all kinds of things such as whether some prisoners are more likely to re-offend, whether a welfare recipient should get a state loan, or whether to reject a job applicant. And the process by which they arrive at these conclusions is often enormously complicated, using mathematical algorithms that even the people who programmed them have great difficulty understanding.

Natural justice norms, particularly the right to a reasoned order (*audi alteram partem*), are violated when the state employs Black Box AI for

administrative or criminal decisions. Any legal procedure must be fair, just, and reasonable, according to Article 21 when read in conjunction with Article 14. An automated decision is intrinsically arbitrary if it cannot be justified, audited, or logically challenged. In *E.P. Royappa v. State of T.N.* (1974)²⁵, the Supreme Court made it clear that "equality is antithetic to arbitrariness." Therefore, it is a clear breach of constitutional due process to assign sovereign state functions or crucial administrative decisions to an inexplicable algorithm.

4.2 Predictive Policing: The Codification and Automation of Prejudice

One of the state's most concerning uses of AI is "Predictive Policing." Several Indian state police forces are currently experimenting with AI software, drawing inspiration from western models (such as the COMPAS algorithm in the US). In order to forecast where crimes will occur (hotspot policing) and who is likely to commit them (person-based predictive policing), these systems examine past crime data, CCTNS (Crime and Criminal Tracking Network & Systems) records, socioeconomic indicators, and demographic data.

While the stated goal of preventing crime is not questionable, the tools to achieve it are. The issue is that predictive policing software is inherently biased. The artificial intelligence is trained on data that reflects past decisions made by policemen. If there was systematic discrimination against a group of people for decades, it would be reflected in the policing algorithm.²⁶

For example, if one racial or ethnic group is historically more likely to be subject to police presence and unwarranted arrest, the AI will identify this as a "high crime area." This means that more police will be deployed there, resulting in more arrests, which the algorithm will use as a basis for further arrests, creating an unbreakable loop of discrimination that is masked under the "scientific" veil of mathematics—otherwise known as "mathwashing."

4.3 The Violation of Article 14 and Article 15 (Indirect Discrimination)

The use of biased algorithms by the state violates article 14, which protects all persons under the law from being discriminated against. If the biased algorithm is used to target specific groups of people for state surveillance or deny them services by inaccurate data models, it is discriminatory and unjust.

Additionally, the state is expressly forbidden by Article 15 from discriminating against any person solely on the basis of race, religion, caste, sex, or place of birth. AI proponents frequently claim that algorithms are "colorblind" or "caste-blind" since specific data items like "religion" or "caste" are not included in the dataset. But sophisticated algorithms are quite good at finding "proxy variables" that strongly correlate with protected identities, including pin codes, food patterns, educational institutions, or surnames.²⁷

If an AI denies a state service, flags a resume, or tattles to police via a proxy (pin code) that happens to represent a Dalit or Muslim-majority neighborhood, that is already indirect discrimination. In *Nitisha v. Union of India* (2021)²⁸, Supreme Court acknowledged the principle of indirect or systemic discrimination. Any criteria that may seem neutral but has a differential impact on the rights of a protected class violates the Constitution. AI systems are likely to do exactly that, committing systemic proxy discrimination, which is a clear violation of Article 15.

4.4 The Need for "Algorithmic Impact Assessments" (AIA)

The state must operate in a fair, reasonable, and discrimination-free manner, as the Supreme Court has repeatedly stressed. However, the scope, intricacy, and imperceptibility of algorithmic prejudice are too much for conventional anti-discrimination rules, which were written with human purpose in mind.

Indian jurisprudence needs to change quickly in order to incorporate AI within the constitution. Before any state agency uses AI for public services or law enforcement, the law must recognize a statutory "Right to Explanation" (as found in the EU GDPR) and require thorough Algorithmic Impact Assessments (AIA). The state would be legally required by an AIA to ensure stringent data minimization, publicly audit algorithms for bias, and ensure that a "human-in-the-loop" maintains final decision-making authority. The algorithmic state threatens to replace constitutional equality with programmed inequity in the absence of these protections.²⁹

5. Corporate Exploitation, Surveillance Capitalism, and the Inadequacy of the IT Act, 2000

While the discussion about the Right to Privacy mostly focuses on the State's actions, the biggest threat in this century is private non-state actors. Tech giants,

search engines, and social media are built on a business model that actively and specifically monetizes human behavior. This trend places a completely different set of challenges in terms of constitutionality and privacy.

5.1 Surveillance Capitalism and the Theft of "Behavioral Surplus"

The modern-day equivalent of neoliberalism is defined by Zuboff as Surveillance Capitalism. For her, the main characteristic of the new economy is that our searches, location data, emotions, and friendships are transformed into a free raw material for new AI systems that seek to harvest a behavioral surplus.³⁰

This surplus is employed to produce highly accurate computerized dossiers that predict user behavior. However, modern AI has progressed past prediction to manipulation. By using deep-learning algorithms (also, an approach which was clarifying illustrated with Cambridge Analytica) and applying "nudging", platforms can, ever so slightly, distort a consumer's choice, influence his emotions, or even change the outcome of an election vote. The Article 21 and Article 19(1)(a) essentially protect decisional privacy and freedom of thought. But when a private corporation's algorithmic might is purposefully employed to subconsciously distort human autonomy and processes, it starts using the people as mere data-producing commodities.³¹

5.2 Data Colonialism and the Loss of Data Sovereignty

In the context of the Global South, especially India, a new form of corporate exploitation is emerging. The term 'Data Colonialism' is being used to describe how huge technology companies, mostly based in the West, appropriate vast amounts of personal data from Indian citizens, processes them with private algorithms in their countries, then sells them back to advertisers and political parties.

The Puttaswamy judgment recognized that informational privacy is an aspect of human dignity; when overseas commercial entities mine the behavioral data of over a billion Indians, it creates a structural asymmetry of power that the Constitution must address to protect the digital sovereignty of Indians. The unidirectional flow of data makes citizens bereft of "informational privacy" and weakens the concept of national data sovereignty.³²

5.3 The Structural Failure of the IT Act, 2000 and the "Consent Fallacy"

For more than twenty years, the legal protection for Indian citizens from corporate data exploitation has been provided by the Information Technology Act, 2000 read with the SPDI Rules, 2011. The provision of Section 43A compensates for the harm caused due to negligence in implementing reasonable security practices while the Section 72A imposes penalty on disclosure of information contrary to a lawful contract.

However, these provisions are hopelessly archaic for the AI era. The IT Act relies on a 'notice and consent' framework, which is structurally broken in today's environment. Consent in the digital ecosystem is obtained through opaque, excessively long 'Terms of Service' designed as 'take-it-or-leave-it' (adhesion) contracts. In addition, the context of Machine Learning, users cannot give 'informed consent' as even the Data Fiduciaries do not know what unforeseen correlations their algorithms might find from the data collected.³³ This illusion of consent is weaponised by corporates to circumvent the fundamental right to privacy.

5.4 The "Safe Harbor" Dilemma under Section 79

Another problem in the IT Act is the total immunity provided to tech platforms under Section 79. They have been treated as 'neutral intermediaries'. However, when it comes to AI platforms, this neutrality is compromised since they influence (or are programmed to promote) the content that appears on their platforms. As such, such platforms can no longer claim to be merely hosts of information and should be treated as publishers. By giving absolute immunity (overriding even publisher liability), the Bill allows such entities to capture user data and use AI tools for manipulation without any accountability.³⁴

5.5 Horizontal Application of Article 21: The WhatsApp Privacy Case

Fundamental rights under Part III of the Constitution are typically only enforceable vertically, that is, against the "State" (Article 12). But today, nation-states are not as powerful in terms of infrastructure as digital monopolies.

To bridge this huge accountability gap, constitutional jurisprudence needs to adapt to recognize the horizontal application of Article 21 against private technology conglomerates operating in the digital space. In a landmark ruling, the Supreme Court has opened the floodgates to such an

interpretation. In the much-anticipated *Kaushal Kishor v. State of U.P.* (2023)³⁵ case, it held that fundamental rights under Articles 19 and 21 can now be enforced against non-state actors.

Presently, before a Constitution Bench of the Supreme Court in *Karmanya Singh Sareen v. Union of India* (the WhatsApp Privacy Case)³⁶, is this very tension between corporate data policies and constitutional rights. The petitioners argue that mandatory data sharing between WhatsApp and Meta (Facebook) violates the informational privacy of millions of Indians. The courts definitely need to interfere here. If the Court holds that corporate algorithmic profiling and forced extraction of data violate Article 21, it would amount to recognition of an important argument that the Right to Privacy cannot be contracted away by coercive digital agreements.

6. The Digital Personal Data Protection (DPDP) Act, 2023: A Constitutional Appraisal in the AI Era

The Puttaswamy judgement that recognised informational privacy as a fundamental right requires an equally robust forward-looking legislation to regulate the flow of digital data. After a decade-long wait beginning with the Justice B.N. Srikrishna Committee Report in 2018, the Parliament passed the Digital Personal Data Protection (DPDP) Act in August 2023. With the introduction of this Act, India joins the formal data economy. However, whether it can protect Article 21 from the fast advancing opaque capacities of Artificial Intelligence needs a constitutional scrutiny.

6.1 Positive Milestones: Formalizing the Data Ecosystem

The DPDP Act refers to the legal relationship between the individual (Data Principal) and any organization (Data Fiduciary) that processes their data. Its objective is to place data processing on the basis of consent that is explicit, informed and unconditional (Section 6). It advocates for the introduction of "Consent Managers" to help users in dealing with complicated digital agreements and of DPB to adjudicate breach of contract and impose heavy monetary penalties. In short, it aims to tighten the legal framework of the Supreme Court's informational privacy mandate.

6.2 The Dilution of Consent and "Certain Legitimate Uses"

The Act overlooks many realities of data mining involving AI despite using these essential measures. Under Section 7, a person's data can be processed without consent for "certain legitimate uses." This includes any data which the principal voluntarily offers, as well as any data that is used to distribute state welfare. Also, data which is relied upon for the provision of medical emergency services.

What is often overlooked is that AI technology is trained using "scraped data". This is data you voluntarily share for one specific benign purpose (like a social media "interaction"). It gets reused, though, for something else entirely. This is what happens when the data is reused to train a large algorithm (like Generative AI or a predictive profiling engine). It all happens without your consent. The Act creates a major loophole by weakening the concepts of 'purpose limitation' and 'data minimization' that were at the core of the 2018 Srikrishna Committee draft. The weakening allows AI developers to harvest and process "publicly available" personal data without regard for consent protocols which severely undermines the decisional privacy of citizens.³⁷

6.3 The Orwellian Exemption: Section 17 and State Surveillance

Section 17, which gives the Central Government broad administrative authority to exempt any of its agencies from the Act's obligations, is the DPDP Act's most serious constitutional weakness. Broad, ill-defined justifications like "sovereignty and integrity of India," "security of the State," and "maintenance of public order" may be used to invoke these exclusions.³⁸

When read in context of AI and mass profiling, Section 17, by creating a dangerously dual ecosystem of highly regulated private sector enterprises as well as completely unregulated state surveillance apparatus, becomes a perilous tool to enable indefinite, algorithmic, digital surveillance of every citizen. By creating a categorical exemption for state law enforcement and intelligence agencies from obligations of purpose limitation, data minimization and obligation to delete, the Act creates a perverse incentive to develop and deploy more and more sophisticated predictive policing tools which go completely unreviewed by any oversight mechanism thus representing a direct assault on the right to privacy guaranteed under Article 21 and endangering the very existence of democratic republic as we know it.

Puttaswamy judgment, specifically the 'least restrictive measure' proportionality test, ought to be applied with a view to prevent precisely such an outcome.³⁹

6.4 The Missing "Algorithmic Due Process" and Automated Decision-Making

Perhaps the biggest omission in the DPDP Act is that it does not mention anything about Artificial Intelligence, algorithmic profiling, and automated decision-making in general. Compare this to the EU's GDPR, which in its Article 22 explicitly states the rights of an individual "not to be subjected to a decision based solely on automated processing, including profiling," while the Indian Act makes no mention of such rights.⁴⁰

If a state algorithm wrongly denies a marginalized citizen his food rations or an AI classifies a citizen as a criminal risk, the DPDP Act gives no statutory "Right to Explanation" or human intervention. Due to the absence of a legal obligation to make algorithms auditable, transparent and free of bias, the DPDP Act proves to be substantially inadequate to protect the substantive due process rights guaranteed by Article 21. The DPDP Act tries to regulate the data but completely neglects the algorithm which processes and weaponizes it.

6.5 Independence of the Data Protection Board (DPB)

The enforcement mechanism is also a matter of great concern as it poses constitutional questions about separation of power and the doctrine of fairness. The Data Protection Board (DPB) is the adjudicating body meant for taking punitive action against data breaches. However, according to the Act, the Central Government has exclusive powers over the appointment and removal of the chairperson and board members.⁴¹

When a State is the largest data fiduciary in the country and one of the primary deployers of AI surveillance machines (such as the CCTNS and Facial Recognition Systems), a regulatory board that lacks functional and financial independence from the executive cannot act as an impartial authority in protecting the rights of citizens from the state's excesses.

7. Global AI Jurisprudence: A Comparative Analysis (The EU AI Act vs. India)

The combination of Artificial Intelligence and fundamental rights poses a global jurisprudential

crisis. The regulation of algorithmic state by various jurisdictions tests India's constitutional preparedness with multiple perspectives, including artificial intelligence. The stark dichotomy between the European Union's proactive and rights-based strategy and India's reactive and innovation-led stance reveals noteworthy shortcomings in India's legal regime in the context of Article 21.

7.1 The European Union: A Proactive, Rights-Centric Paradigm

The European Union (EU) is leading the way in managing the digital economy by shielding citizens from undue oversights by capitalist innovations or the State. The General Data Protection Regulation (GDPR) and the newly proposed EU Artificial Intelligence Act (AI Act) will govern the area.

The GDPR and Algorithmic Due Process Essay: The essay on the GDPR and algorithmic due process describes the former as a data protection law coming into effect in 2018 as well as more than that. Moreover, it deals with automated decision-making issues. Most importantly, Article 22 of the GDPR states that an individual has the right "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her." In other words, use of "Black Box" AI in critical sectors is unlawful under the GDPR as there is a "Right to Explanation" and human intervention.⁴²

Building on the GDPR, the EU has introduced the Artificial Intelligence Act (2024), which introduces the world's first legal framework to regulate AIs directly and specifically. The EU AI Act adopts a strict "Risk-Based Approach" that categorizes AI systems based on the level of risk they pose to fundamental rights.

- 1. Unacceptable Risk (Banned):** AI systems that pose a significant risk to human life and livelihood are prohibited. This includes social scoring systems by governments, and real-time remote biometric identification (such as facial recognition) by law enforcement in public places, effectively forbidding the state panopticon.⁴³
- 2. High Risk:** AI systems that are applied in critical infrastructure, workforces, education, law enforcement (judicial evaluation of evidence reliability), etc., are subject to strict regulation. Such systems are required to undergo mandatory conformity assessment procedures, algorithmic auditing, and the implementation of appropriate human oversight before deployment.

- 3. Limited and Minimal Risk:** Less stringent transparency requirements apply to systems like chatbots and spam filters, which mainly make sure users are aware that they are engaging with a machine.

7.2 The Indian Approach: Innovation Over Regulation

As opposed to the EU's rights-based legislation, India does not currently have any specific parliamentary statute regulating Artificial Intelligence. India's approach has been to embrace technology, ease of doing business, and state efficiency, while being somewhat dismissive towards the active protection of the Article 21.

NITI Aayog's Non-Binding Guidelines: The primary policy documents, which regulate AI in India, are NITI Aayog's reports (the Government's public policy think tank). In 2018, it released the "National Strategy for Artificial Intelligence," and "Responsible AI for All" working documents were released in 2021. The reports acknowledge the risks of algorithmic bias, opacity, and privacy violation but serve only as advisory guidelines and ethical frameworks.⁴⁴ They have no statutory force, and the State and private corporations cannot be penalized for violating them.

The DPDP Act Vacuum: As discussed in Section 6, while the Digital Personal Data Protection (DPDP) Act, 2023, seeks to regulate the underlying data, it remains completely silent on the regulation of the algorithms processing the data. It does not have an equivalent of GDPR's Article 22, providing no statutory 'Right to Explanation' or protection against automated profiling. While the EU AI Act explicitly bans real-time facial recognition by the state in public places, the Indian government is busy funding and using the National Automated Facial Recognition System (NAFRS) without any legislative guardrails.

7.3 The Constitutional Imperative for India

The difference between the EU and India is a constitutional problem. India is relying on an outdated and inadequate law, the IT Act 2000, and failing to develop a specific legislation for AI, leaving the Right to Privacy under Article 21 exposed to the vagaries of capital and state power. The failure to create an Indian counterpart to the EU's AI Act, which would classify predictive policing and mass biometric surveillance as unacceptable risks, leaves India vulnerable to the whims of individual executives.⁴⁵

The Indian judiciary, inspired by the visionary contours of the Constitution, must realize that guidelines on technology are inadequate. Instead, a rights-based, global best practice-inspired, yet contextually sensitive AI jurisprudence is an imperative constitutional obligation.

8. Conclusion and Recommendations: Forging a New Constitutional Paradigm

Artificial Intelligence and mass data processing is not only a technological revolution but also one of the most critical constitutional challenges of the 21st century. The Right to Privacy—which is recognized as an intrinsic part of human dignity and individual freedom under Article 21 of the Indian Constitution—is under threat both from State-sponsored algorithmic surveillance and corporate data mining.

This research paper has illustrated that the "notice-and-consent" approach which is embedded in the traditional legal frameworks like the Information Technology Act, 2000, the new Digital Personal Data Protection (DPDP) Act, 2023 or the very concept of "Black Box" and deployment of "predictive policing" that reproduces historical prejudices or the exemption of "State's intelligence agencies" from the purview of DPDP, 2023, altogether negate the very idea of "procedure established by law" and "proportionality test" as enshrined by the Supreme Court in its landmark Puttaswamy judgment.

If it is to be a living document that protects the citizens, the Constitution needs a complete jurisprudence upgrade. The Right to Privacy should no longer be interpreted through the lens of territorial integrity but instead be reinterpreted to impose obligations on information flows, algorithmic transparency, and data sovereignty.

Recommendations for a Future-Proof Jurisprudence

The following legislative and legal changes are critically necessary to guaranty that the Right to Life and Personal Liberty endures in the algorithmic state:

- 1. Enactment of a Specific AI Regulation Statute:** India needs an AI Act, separate from data protection laws, inspired by the EU AI Act, which adopts a "Risk-Based Approach" to governing high-level artificial intelligence. The Act should require conformity assessments of high-risk AI systems used in law enforcement, welfare distribution, and the judiciary, and prohibit

unacceptable risks (real-time facial recognition in public places and social scoring).

2. **Mandatory Algorithmic Impact Assessments (AIA):** The law must require that every use of algorithms by the State for public services and law enforcement be subjected to an Algorithmic Impact Assessment to demonstrate that they do not have an unfair discriminatory effect on vulnerable populations (and thus violate Articles 14 and 15).
3. **Establishing a Statutory "Right to Explanation":** The Constitution secures the right against the arbitrary interference of the state. Consequently, the law must explicitly recognize the right of an individual to demand a human understandable explanation for any automated decision that significantly impacts his or her legal rights, liberties, or access to state resources, effectively banning "black box" governance.
4. **Amendment of the DPDP Act 2023:** The broad and disproportionate exemptions provided to state agencies under Section 17 of the DPDP Act have to be significantly narrowed. Any processing of personal data by the state for reasons of national security has to be subjected to judicial oversight and have to adhere to the principles of purpose limitation and data minimization.
5. **Reading "Algorithmic Due Process" into Article 21:** The Supreme Court Of India must interpret Article 21 to explicitly include and mandate 'algorithmic due process', and 'digital autonomy'. A framework which seeks to hold State and potent non-State actors accountable, where technology empowers and doesn't erode human dignity.

Final Thought

The age of Artificial Intelligence brings the ultimate constitutional predicament. According to framers of the constitution, India was to be a republic of her citizens, where the State was to be for the people and was to be ruled by law. If the judiciary and the legislature do not aggressively fail to take up the task of defending the Right to Privacy today, it would in future only be a legal fiction, superseded by code, algorithmic dictates, and the cold efficiency of the machine. The next moment the beauty that lies in the essence of communication of idea in Article 21 and its expansive interpretation would be diluted if the state does not take it up with urgency.

References

1. *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
2. Schwab, K. (2017). *The Fourth Industrial Revolution*. Crown Business. (Discussing the profound societal shifts caused by AI, robotics, and the Internet of Things).
3. Domingos, P. (2015). *The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World*. Basic Books.
4. A metaphor used by Jeremy Bentham to describe a prison with many inmates who are constantly under the view of a watchman, who himself remains invisible to them.
5. Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison*. Pantheon Books.
6. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
7. Solove, D. J. (2004). *The Digital Person: Technology and Privacy in the Information Age*. NYU Press.
8. *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300
9. *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295.
10. *Ibid.*
11. *Gobind v. State of M.P.*, (1975) 2 SCC 148.
12. 381 U.S. 479 (1965).
13. *Malak Singh v. State of Punjab & Haryana*, (1981) 1 SCC 420.
14. *R. Rajagopal v. State of T.N.*, (1994) 6 SCC 632.
15. *Selvi v. State of Karnataka*, (2010) 7 SCC 263.
16. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
17. *Ibid.* (Justice Chandrachud, discussing the nuances of Informational Privacy, data sovereignty, and its critical importance in an increasingly digitized society).
18. Barak, A. (2012). *Proportionality: Constitutional Rights and their Limitations*. Cambridge University Press.
19. *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301.
20. Harcourt, B. E. (2007). *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age*. University of Chicago Press.
21. Ministry of Home Affairs, Government of India. (2019). *Request for Proposal for National Automated Facial Recognition System (NAFRS)*. National Crime Records Bureau.
22. *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.

23. Richards, N. M. (2013). *The Dangers of Surveillance*. Harvard Law Review, 126(7), 1934-1965.
24. *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.
25. *E.P. Royappa v. State of T.N.*, (1974) 4 SCC 3.
26. O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown.
27. Barocas, S., & Selbst, A. D. (2016). *Big Data's Disparate Impact*. California Law Review, 104, 671.
28. *Lt. Col. Nitisha v. Union of India*, (2021) 15 SCC 125.
29. Reisman, D., Schultz, J., Crawford, K., & Whittaker, M. (2018). *Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability*. AI Now Institute.
30. Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.
31. Susser, D., Roessler, B., & Nissenbaum, H. (2019). *Technology, autonomy, and manipulation*. Internet Policy Review, 8(2).
32. Couldry, N., & Mejias, U. A. (2019). *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford University Press.
33. Solove, D. J. (2013). *Privacy Self-Management and the Consent Dilemma*. Harvard Law Review, 126(7), 1880-1903.
34. Citron, D. K. (2007). *Technological Due Process*. Washington University Law Review, 85, 1249.
35. *Kaushal Kishor v. State of Uttar Pradesh*, (2023) 4 SCC 1.
36. *Karmanya Singh Sareen v. Union of India*, SLP (C) 804/2017 (Pending before the Supreme Court of India).
37. Report of the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna. (2018). *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*.
38. The Digital Personal Data Protection Act, 2023, Section 17(2)(a).
39. Internet Freedom Foundation. (2023). *Analysis of the Digital Personal Data Protection Act, 2023*.
40. Regulation (EU) 2016/679 (General Data Protection Regulation), Article 22. (Contrasting the robust algorithmic safeguards in the EU with the legislative void in India).
41. The Digital Personal Data Protection Act, 2023, Sections 19 & 20.
42. Regulation (EU) 2016/679 (General Data Protection Regulation), Article 22. (Establishing the right against automated individual decision-making).
43. Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM/2021/206 final.
44. NITI Aayog, Government of India. (2021). *Responsible AI #AIForAll: Approach Document for India - Part 1: Principles for Responsible AI*. (A conceptual framework lacking statutory enforcement mechanisms).
45. Basu, A. (2021). *We Need a Law, Not Just Guidelines, to Regulate Facial Recognition Technology in India*. Internet Freedom Foundation.

Disclaimer/Publisher's Note: The views, findings, conclusions, and opinions expressed in articles published in this journal are exclusively those of the individual author(s) and contributor(s). The publisher and/or editorial team neither endorse nor necessarily share these viewpoints. The publisher and/or editors assume no responsibility or liability for any damage, harm, loss, or injury, whether personal or otherwise, that might occur from the use, interpretation, or reliance upon the information, methods, instructions, or products discussed in the journal's content.
