Page 903 - 914 **DOI:** *https://doij.org/10.10000/IJLMH.1112086*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 3

2026

Whether AI-Driven Surveillance Mechanisms and Decision-Making are Compatible with the Right to Privacy and Due Process under the Indian Constitution?

SONALI SHARMA* AND DR. ARUN SHARMA**

ABSTRACT

The development of Artificial Intelligence has brought about major transformations in the field of Technology, Healthcare, Education, finance and Governance. The recent trends suggest a massive shift in the use of AI from being a techno-centric, conventional mechanism to a contemporary solution to all modern-day needs. The growth of AI is prima facie based on the advancement of Human intelligence and its desire to turn every facet to transform challenges into major revolutions. There is no denying the fact that AI has been developing the potential of thinking and processing on its own without any human interference in the near future. However, the idea of bringing about an AI revolution has, in itself, brought forward many unforeseeable challenges to be addressed. Innovations in the field of Artificial Intelligence are rising on an alarming scale, and it is an undisputed fact that development should not compromise individual identity and autonomy, but the large-scale use and growing dependence on AI have led to the introduction of mechanisms like Algorithmic Governance and AI-driven surveillance systems.

This paper examines such contemporary challenges posed by the rise of AI-driven surveillance against the digital liberty and fundamental right to Privacy of citizens at large as guaranteed by virtue of Articles 14, 19 and 21 of the Constitution of India. The study adopts a Doctrinal methodology drawing emphasis upon the Constitutional Framework, Statutory analysis and Judicial Opinions, focusing on analysing the adequacy of the present laws in dealing with AI-based Surveillance.

Keywords: *AI Surveillance, Privacy, Algorithmic Governance, Indian Constitution, Biometric Data, Facial Recognition*

I. INTRODUCTION

Artificial Intelligence is being significantly adopted on a global scale to conduct various crucial

* Author is a Student at Amity Law School, Amity University Madhya Pradesh, India.
** Author is an Associate Professor at Amity Law School, Amity University Madhya Pradesh, India.

 [ISSN 2581-5369]

activities like decision-making, policing, and Surveillance. The AI technology has had its own journey, tracing its origin back to the 1930s, which brought forward the concept of "Thinking Machines" and the idea of development of Artificial Neurons resembling the functioning of a Human Brain, which laid the groundwork for the development of Artificial Intelligence. However, on the other hand, AI today has also become one of the major reasons of infringement of the Digital Privacy and Digital autonomy of the Global Population. In the Indian context, AI has been a recent phenomenon and the Indian laws are thus rather more unequipped and inadequate in comparison to its Global partners. The greatest challenge that AI poses against the Indian Legal system is its inefficiency to predict and identify the possible uses of AI-based models and the level of harm they can cause by their unregulated use. Algorithmic profiling or AI-based surveillance and monitoring, for example, are certain such uses that have caused greater harm than adding value, as they utilise the Digital Footprints to label individuals, which are in clear violation of their fundamental rights guaranteed under Articles 14, 19 and 21 of the Constitution of India. This raises a significant question as to whether individual liberty and Digital Privacy be compromised for giving way to every technological innovation?

AI Surveillance refers to the vigilance or monitoring conducted by digital detectives, like computer software, with the capability to work around the clock. These can be distinguished from traditional systems like CCTV monitoring, which were subjected to limitations owing to the fatigue and stress caused to the observer, making them comparatively slow. These newly developed systems work as a contemporary solution to such problems and are also backed by computer intelligence, which helps distinguish actions, identify and analyse behaviour, and accurately spot unusual patterns, thus simplifying complex procedures and Human-made errors. Algorithmic Governance, on the other hand, corresponds to the use of AI algorithms and automated data-driven systems for making decisions to govern and regulate the conduct of People and systems. It encompasses activities like large-scale data collection, surveillance, profiling or predictive analysis to monitor and regulate the behaviour of individuals in order to enforce law and order in society. Biometric Data is a digital record of a person's unique physical, biological or behavioural characteristics used to verify or authenticate a person's identity. Example- Fingerprints, Facial recognition data, DNA profiles, Walking pattern etc. Facial Recognition is a category of Biometric data, and the Facial Recognition Technology (FRT) helps in identifying or verifying people by analysing their features from images or video data.

In the context of the Indian scenario, there are several recent models that utilise AI as a means to speed up and simplify government functions. The use of Facial Recognition Technology

 [ISSN 2581-5369]

(FRT) and CCTV cameras enhanced with AI capabilities during the Prayagraj Maha Kumbh to send alerts in case of a surge in any one section of the festival city, and to find lost persons; or the use of AI-driven surveillance systems in Mumbai and Pune with the ability to perform facial recognition and behavioural analytics during mass processions or Ganpati Visarjan. Similar systems have also been utilised by the Delhi Police during Independence Day for conducting tasks like abandoned object identification and people count. It is an undisputed fact that every nation should work on its technological soundness and ability to cater to the rapid changes arising globally in the field of technological advancements to stay updated. Utilisation of such AI-mechanisms is one such technological advancement that India has been exploring, but this in turn raises a question as to whether the nation's Cyber Security and Digital Privacy Laws suffice the present-day need of Protection against such potential threats raised by AI?

II. COMPARATIVE ANALYSIS OF GLOBAL LEGAL FRAMEWORKS

On a Global scale, it can be observed that various Jurisdictions have been stressing the need for the formation of Specific laws to deal with AI-based operations.

A. The EU Artificial Intelligence Act

The EU Artificial Intelligence Act is one such example of a comprehensive framework introduced to regulate the use of AI. The Regulation categorises risks associated with the use of AI into Unacceptable Risks and High Risks categories on the basis of the risks posed to the users, and also lays down certain Transparency requirements to be adhered to by Platforms that do not fall under either of the two stipulated categories. The Act was introduced in April 2021, as the EU's first regulation on Artificial Intelligence and aims to regulate the use of AI against its potential harm to the fundamental rights of its citizens and at the same time to promote and encourage AI-based Startups and Innovations. The High Risks Category stipulated under the regulation comprises of AI systems that negatively affect the fundamental right of the citizens, like Systems having a potential negative impact on Education, Law enforcement, Employment, Border control management and asylum, etc. On the contrary, the Unaccepted Risks category lays down the banned AI applications like Systems working in the field of Cognitive Behavioural manipulation of people, Biometric identification and classification of people, real-time and remote biometric identification systems[1] and facial recognition systems in public places, etc. However, there are certain exceptions made under this category with respect to law enforcement purposes, wherein the Real-time Biometric Identification and Facial recognition

[1] European Parliament, "EU AI Act: First Regulation on Artificial Intelligence", available at: [https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence] (last visited on April 24, 2026).

 [ISSN 2581-5369]

may be allowed in certain serious cases.

Apart from the EU AI Act, the European Union General Data Protection Regulation (GDPR is another essential piece of legislation that governs the Privacy and flow of Digital Personal Data in the Digital era. Enforced on May 25, 2018, the GDPR has proven to be a significant step towards promoting and regulating Digital Systems involving Biometric Identification, Facial Recognition, Behavioural tracking and automated decision-making. The act draws an emphasis upon a "consent-based regime" of data processing, imposing a statutory obligation on those processing Digital Personal Data to obtain "Consent" from the Data Subject. Biometric information is categorised as a special category of personal data under Article 9 of the act. It works on the founding pillars of Data Minimisation and Purpose Limitation making, thereby emphasising on greater scrutiny of surveillance mechanisms. However, the act proves insufficient and inadequate on several parameters like- Ambiguity around what would be classified as Legitimate interest, Complexity in the working of AI-based models, enforcement upon State Surveillance exemptions etc. In certain parameters, the act resembles the UK GDPR and India's Digital Personal Data Protection Act. The act still fails to provide an immediate recognition and remedy to AI-based surveillance.

B. The Principle-based Approach: UK

Unlike the EU, the UK has no dedicated Act or legislation in place to regulate the use of AI. The UK greatly relies on a non-statutory framework as published by the Government on a White Paper in March 2023, which consists of five core AI Principles i.e. Safety, Security and Robustness, Transparency, Fairness, Accountability, Contestability and Redress[2]. Furthermore, in the context of the UK's policy regime regulating the use and impact of AI, no such "AI regulators" have been introduced; rather, the various authorities and bodies, such as the FCA and ICO would be responsible for regulating AI in their own sectors. It has placed emphasis on self-regulation by businesses and regulators by ensuring compliance to the Principles rather than imposing any Legal restrictions. As far as the Current status is concerned, the UK plans on introducing a well-structured Legal Framework i.e the Artificial Intelligence (Regulation) Bill, as was reintroduced in the House of Lords in March 2025 and codify all five Principles into binding legal duties[3] under it so as to ensure their strict compliance by law.

Furthermore, with regard to the use of Personal data and Biometric information, the UK has

[2] Valeria Gallo and Suchitra Nair, "The UK's Framework for AI Regulation: Agility is Prioritised, but Future Legislation is Likely to be Needed", available at: [https://www.deloitte.com/uk/en/blogs/ecrs/the-uks-framework-for-ai-regulation.html] (last visited on April 24, 2026).

[3] Zlatko Delev, "UK AI Regulation: Current Status and Outlook", available at: [https://gdprlocal.com/uk-ai-act/] (last visited on April 24, 2026).

 [ISSN 2581-5369]

implemented 2 major regulations i.e. the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. In order to process or use any personal data any entity has to strictly observe the "Data Protection Principles" as laid down under the regulations unless any exception applies. The Act guarantees rights to Data Subjects in relation to the processing of their personal data and also imposes certain restrictions on acts like unauthorised profiling and automated decision-making. However, as far as surveillance is concerned, a major drawback is not assigning a specific meaning to what would be deemed a national security interest. This overpowers the authority to label any act in the interest of Public safety and national security, and thereby processes the personal data of the data subjects without obtaining their prior consent.

C. The Indian Approach

The Indian Legal Framework, like the UK, has no dedicated Statute or Regulation governing AI-based Surveillance, and the existing Cyber Security Laws and Data Protection Laws are obsolete in the sense that they fail to recognise the concept of Artificial Intelligence in its strict sense. At present, the existing Cybersecurity and Data Protection Laws, i.e. the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, are utilised to address any offences related to Cybersecurity or Data Breach by any such AI-mechanism. The Digital Personal Data Protection Act, 2023 was particularly introduced with an aim to regulate the processing of Personal Data and to penalise actions violating the Digital Privacy of any individual. However, it is to be noted that the act fails to recognise the prevalent technology and novel means of violation of Privacy that have come forth by the birth of Artificial Intelligence. Algorithmic Governance, Digital Profiling, AI-surveillance, Automated decision making, and Generative AI are certain contemporary concepts that the new DPDP regime fails to account for. While the act emphasises obtaining "consent" from the Data Principal before the processing of their personal Data, on the contrary, it also provides wide powers to the State to utilise the personal data of individuals for promoting "National Interest". The act remains silent as to what action of the State would be classified or labelled as "National Interest", thereby leading to uncertainty and ambiguity in the provision, leading to overpowering the State by entrusting it with a massive amount of digital personal data of the citizens at large.

III. THE CONSTITUTIONAL DIMENSIONS OF AI IN INDIA

Artificial Intelligence or AI-based Surveillance, though, does not find any express mention in the Indian Constitution; however, various Judicial pronouncements can be referred to so as to

understand the Indian approach to Privacy. In simple terms, Privacy is the right to be left alone[4]. Furthermore, Article 21 of the Constitution of India talks about the Fundamental right to Life and Personal Liberty of the citizens, and recognises "Privacy" as a part of Right to Life, encompassing their digital privacy as well. The Judgment pronounced by the Hon'ble Supreme Court has been a landmark Judgment wherein the Court has held that the Fundamental right to life and personal liberty guaranteed under Article 21 shall also include the right to privacy. It was also specifically stated that Privacy is intrinsic to dignity, liberty, autonomy, and informational self- determination[5]. The Right to Privacy is an integral part of the right to life and a cherished constitutional value, thus making it essential that Human beings be allowed domains of Freedom that are free of any Public scrutiny unless they act unlawfully, the Union of India should not take an adversarial position when the fundamental rights of citizens are at threat[6]. Herein, even AI-driven behavioural profiling, metadata tracking, Facial recognition and other forms of AI-based surveillance are direct intrusions into the informational privacy of the citizens.

Though the Judgments make no specific mention of AI Technology, they can be resorted to understand the Judicial opinion regarding Digital Privacy and surveillance mechanisms and can be applied in cases pertaining to violations of Privacy by such AI Platforms. Another such essential piece of testimony against unregulated surveillance was provided in the Manohar Lal Judgment, wherein the court had recognised that the Acts like surveillance and spying are an infringement of the right to Privacy of the citizens except when done with the objective of securing life, liberty, and Security. It was also stated therein that indiscriminate spying cannot be allowed, and such surveillance or spying by means of the usage of technology shall be based on evidence and shall be resorted to only when absolutely necessary[7].

However, no such test to establish what would amount to "necessity" was provided by the ruling. These judgments establish the duty of the State to produce reliable evidence showing absolute necessity to adopt such projects, before encroaching upon the Fundamental Right to Privacy of the Citizens. Furthermore, the Judiciary is empowered to keep a check on such State's actions so as to ensure that surveillance is justifiable on National Security grounds[8], unobtrusive and within bounds as excessive surveillance falling beyond limits prescribed by the rules shall entitle a citizen to the Court's protection.[9] This depicts the role of the Judiciary in

[4] Navtej Singh Johar v. Union of India, (2018) 10 SCC 1.
[5] K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.
[6] Ram Jethmalani v. Union of India (Black Money Case), (2011) 8 SCC 1.
[7] Manohar Lal Sharma v. Union of India, (2023) 11 SCC 401.
[8] PUCL v. Union of India (Telephone Tapping, 1997).
[9] Malak Singh v. State of P&H, (1981) 1 SCC 420.

 [ISSN 2581-5369]

the protection and promotion of Digital Privacy and their duty to regulate the State's actions to curb activities like surveillance to ensure data safety.

The plethora of Judgments passed by various courts provides a clear picture as to the judicial perspective on privacy. One such landmark judgment was passed in the Aadhar case, wherein the Hon'ble Supreme Court of India, while observing the impact of profiling and processing of Biometric metadata had clearly stated that "Profiling does impact individual behaviours and in the Modern Era, the basic essence of privacy protection is that there should be provable guarantees that the data cannot be used for any purpose for which such data processing has not been approved. Also, in a national-level identification system, individuals' credentials are at risk, as they are prone to becoming an easy target for anyone looking to cause serious damage, thereby causing damage to individual autonomy.

Further, it was also observed that Data Collection, usage and storage require adherence to the principles like obtaining consent, indicating purpose and ensuring compliance to storage limitations, data differentiation, data exception, data minimisation, observing substantive and procedural fairness and safeguards, maintaining transparency, data protection and security and only after strictly observing these principles can a State successfully discharge the function of proportionality while affecting the Privacy of its citizens[10]. This Judgment emphasis a need for a consent-based framework for the processing of Digital personal data so as to avoid any risks associated with large-scale data storage and handling. This step also provides a solution to the challenge of Data Processing by unidentified users or Malicious actors.

Another constitutional standard of "Privacy" is the potential impact of any action on the Freedom of Speech guaranteed under Article 19(1)(a) of the Constitution of India. The unauthorised or unregulated surveillance by any Public/ Private authority or by the State acts as a "chilling effect" on free expression. All the members of a society should be able to form their own beliefs and communicate them freely, thereby establishing the fundamental principle of "People's Right to know[11]. Surveillance hinders communication or expression amongst individuals by making them conscious about being consistently under vigilance, thereby acting as a "chilling effect" even on Private communications. What determines which communication or activity is to be surveilled, and what would constitute the limit? The FRT Technology, so developed, relies on AI to identify or verify a person by analysing facial features from any available records or digital database and produces a match or probable identity. However, such

[10] K.S. Puttaswamy & Anr. (Aadhaar) v. Union of India, (2019) 1 SCC 1.
[11] Indian Express Newspapers (Bombay) (P) Ltd. v. Union of India, (1985) 1 SCC 641.

 [ISSN 2581-5369]

technology cannot be presumed to be completely free from making errors or bias. In such a scenario, who must be held accountable in case of any misidentification, and under what law shall he be governed? Artificial intelligence cannot be said to function on sole reliance on itself, as it is still not developed enough to understand the connection between what is said or done by any individual and the emotional context or other underlying meaning associated with what was said or done by such individual. The state has authority with regard to the utilisation of Personal information or communications, for conducting confidential operations; however, at the same time, the citizens' right to Privacy and expression has to be protected from being abused by the authorities. Also, before settling on any method restricting the freedom of Speech and Expression of any individual, the authorities must assess the existence of any alternative mechanism. A decision curtailing Freedom without an appropriate justification will be Disproportionate[12].

The system is also arbitrary due to a lack of control and transparency, which violates Article 14 of the Indian Constitution, which encompasses the Fundamental Right to Equality. AI-based surveillance and algorithmic governance is violative of Article 14 on the grounds of being Disproportionate, overbroad, and opaque, and also due to the fact that no adequate safeguards or accountability procedures were developed so as to ensure the safety of the rights of the subjects, by giving no specific statutory recognition to Judicial scrutiny in such matters. Arbitrariness and Equality are sworn enemies[13] and subjecting the general public to AI surveillance is in itself manifestly arbitrary, owing to the fact that AI systems feed on available data to make predictions or mere possibilities, which can thus be prone to bias or errors, thus making it unreliable, inaccurate, and defective.

IV. BLANKET OR TARGETED SURVEILLANCE?

Targeted Surveillance refers to the act of monitoring based on reasonable suspicion, security concerns, or lawful authorisation of a specific individual, group or locality. When the AI-based technology is utilised against identified suspects for observing their conduct or communications, then it falls under Targeted Surveillance. It is in stark contrast to Blanket Surveillance, which is the use of AI-based or other technological mediums for facilitating indiscriminate, mass, or generalised monitoring of a large-scale population without individualised suspicion. The classification is based on the size of the targeted population under surveillance. Mass Facial Recognition Systems, Predictive Policing Databases, Automated

[12] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
[13] E.P. Royappa v. State of Tamil Nadu, (1974) 4 SCC 3.

 [ISSN 2581-5369]

CCTV analytics, or Biometric Tracking Systems are all techniques utilised for conducting Blanket Surveillance of the masses.

AI- based targeted surveillance is individual-specific and thus most likely legally sustainable due to being a necessity-based proportionate measure. It further satisfies the three-fold requirement of Privacy as laid down in the Puttaswamy judgment, i.e. 1. Legality, 2. Legitimate Claim, 3. Proportionality, which ensures a nexus between objects and the means adopted to achieve them. It is also time-bound and owes its legal sanctity to an authorised statute, which makes it a bona fide use of such technology. Though it is subject to certain risks related to algorithmic errors and misuse, it is still permissible in certain forms as recognised by the existing statutes, like Section 5(2) of the Indian Telegraph Act, 1885 empowers the government to intercept or detain a message and can even seek a disclosure of such a message in matters concerning Public Safety or Public Emergency. Further, Section 69 of the IT Act, 2000 provides for interception, monitoring and decryption of any information transmitted through a computer resource by the Central or State Government on national security grounds, while Section 69B, respectively, provides for the Monitoring and collection of traffic data or information generated through a computer resource. Though structured formally to emphasise the targeted Surveillance, the overbroad and expansive wording overpowers the government with the ability to conduct large-scale data interception and monitoring, leading to blanket surveillance.

On the other hand, Blanket surveillance by means of AI-based technology is a legally contentious subject, owing to the lack of statutory provisions and old surveillance laws that do not provide for modern AI-powered mass monitoring. Blanket surveillance raises serious constitutional concerns, not only because it is indiscriminate and disproportionate but also due to its significant chilling effect on the Fundamental freedoms of citizens at large. It lacks individualised suspicion, thereby making it prone to profiling and discrimination. The vagueness of such large-scale surveillance mechanisms is further depicted by the fact that an AI-driven survey of the entire population will lead to the creation of a Digital Dossier of Citizens, which is unnecessary and indiscriminate, as it would result in compromising and restricting the Digital Privacy of its Citizens. This would further facilitate unauthorised sources, hackers, and other such malicious actors by serving them with large-scale private/behavioural metadata on a single surveillance record. In the Puttaswamy verdict, the Court has also recognised informational control as one of the connotations of Privacy, stating in its observation that- "Informational control empowers the individual to use privacy as a shield to retain personal control over information pertaining to the person" It was also observed that in cases of national interest state may intervene but it must put into place a legitimate regime that ensures the

 [ISSN 2581-5369]

fulfilment of the threefold requirement. This judgment serves as a major testament to the fact that individuals can exercise informational control over their personal information. However, even so, the Indian Statutory Framework fails to recognise the potential negative impact of AI-based surveillance and Blanket monitoring despite there being several Judicial opinions delivered on the subject.

V. WAY FORWARD

Globally, AI-based systems have been evolving at a rapid pace. This rapid development of AI has presented a Constitutional Dilemma i.e., the need for such technological upgradation to enhance administrative efficiency, and on the other hand, the challenges posed against individuals' privacy, equality, and Freedom of expression by such technology. Notably, at the Constitutional level, we still try to govern AI by means of outdated statutory and regulatory provisions, undermining the fact that such provisions and Judicial opinions were not designed to cater to the problems posed by algorithmic governance. Major Judgments like *KS Puttaswamy*, though, provide an insight into constitutional recognition and protections of Privacy, yet often fail to address the issue relating to the infringement of Privacy by such AI mechanisms.

AI systems are opaque 'BLACK BOX'[14] in nature, highlighting the risks involved in data processing by such mechanisms, as they do not provide insight into the process involved in reaching at the decisions that impact individuals. Due to a higher level of complexity involved, in certain scenarios, even their creators do not fully understand the working of such systems, thereby denoting a higher risk involved in their unregulated operation. In Legal Context, this also undermines "reasoned decision" that is a major principle of natural justice, thereby infringing the individual's right to receive reasons behind certain observations or analyses made by such a system. There are no specific statutory frameworks governing AI surveillance in India since the existing laws, such as the Information Technology Act, 2000, Telegraph Act or the DPDP Act, prove inadequate in assessing the automated decision-making and biometric processing functions governed by AI Surveillance Platforms, thereby raising another challenge as to who bears the accountability. Furthermore, such mass surveillance systems are often prone to misuse and bias as they can be trained or skewed by feeding the system with incorrect or tampered datasets, thereby generating desired results. This nullifies the mindset that AI systems are non-discriminatory owing to no Human interference.

[14] Matthew Kosinski, *What Is Black Box AI?* https://www.ibm.com/think/topics/black-box-ai(last visited May 5, 2026).

The emergence of AI systems has brought forth their utilisation in various dimensions, even encompassing various State operations. Many of the risks involved in greater AI reliance are still unforeseen and cannot be easily anticipated due to its complex nature. Thus, prior steps should be taken to tackle the AI-driven Surveillance operations and algorithmic governance by establishing a structured regulatory framework, particularly dedicated to such technologies. Further, before the introduction of such surveillance systems that have a tendency to affect the Digital Privacy of individuals, proper compliance with the tests laid down under the Puttaswamy verdict must be ensured i.e. the surveillance should be legally sanctioned, proportionate to the object sought to be achieved, and necessary for furtherance of a Legitimate aim. It should also be ensured by the Authorities using such systems that proper disclosure of the surveillance practices shall be made. Mechanisms for proper redressal of claims should also be provided for, to enable those aggrieved with an opportunity to challenge decisions affecting their interests. Independent regulatory authorities should be established and they should be empowered to impose Penalties and punishments for ensuring compliance and eradicating misuse by means of such systems. Stricter consent requirements must be imposed and the use of technologies like FRT should be limited and subjected to a higher level of scrutiny by authorities to determine the underlying motive. Broader exemptions overpowering the State with the authority to process data, the unauthorised storage and use of Personal metadata should also be limited. The Judiciary must ensure proper compliance to such statutory provisions governing the use of AI surveillance and automated decision-making mechanisms, and greater public participation and awareness must be ensured by means of encouraging awareness campaigns on Digital rights, consultations, and transparency reports.

VI. Conclusion

Unrestricted AI Surveillance can lead to serious challenges pertaining to the digital privacy of citizens in the near future. Therefore, it becomes essential to put forth a framework to keep such systems and their controllers under check and ensure safety against unforeseen risks posed by such technology. AI-Surveillance and algorithmic governance techniques today are crossing leaps and bounds, which portrays a greater need to insist upon Public awareness. Awareness shouldn't only be about how such technology can be accessed by users but also about the major risks associated with its blind use. Mechanisms like Blanket surveillance should not be resorted to without proving its proportionality with the harm caused to the fundamental right to Privacy of the citizens at large. Regulatory authorities should be established at various levels, and shall be empowered to hold even the State liable in case of any infringement caused without any justified cause. Greater reliance shall be placed upon empowering people against misuse of such

 [ISSN 2581-5369]

powers rather than subjecting them to Digital authoritarianism.

*****

 [ISSN 2581-5369]