



THE NEW LEVIATHAN: AI POWER, PRIVACY AND INDIA'S SOCIAL DIVIDE- AN ANALYSIS IN THE CURRENT CONTEXT

Aahana Khajuria, Aeera Aroush Khan, Akash Kumar, Garima Rathore, Kashish Kumari, Ritika Das, Shikha Chauhan, Sureely Saxena

Abstract: The Artificial Intelligence era is facilitating 'the new leviathan', that is, digital control and algorithmic dominance. This critically impacts privacy concerns and enhances social inequalities. Therefore, this paper aims to critically interrogate the intersecting relationship between AI and privacy, accelerating social divide and inequalities. It revolves around the AI system in India and primary research conducted over a demographically diverse section of Indians. It showcases how certain factors such as caste, class, income, genders, age groups, literacy, etc., overlaps with the digital inequalities in India. This research has opted for a combination of qualitative and quantitative analysis, in which the primary data has been collected through systematic surveys from different regions of India from over 150 + respondents. The significant findings of this study uncovers that majority of participants affirm that income impacts an individual's knowledge and access to AI, there is a weak correlation between AI understanding and subsequent awareness about AI privacy, and there is a significant association between the age group and understanding of AI. Majority confirms that social media is space where they can witness explicit prevalence of AI using their data, they also assert that protecting user data is a collective responsibility of individual users, government, private companies and international forums, and they also endorse by a majority that education can notably help in spreading awareness about AI usage. This study concludes by endorsing a strong need to strengthen the existing laws by better practical implementation, updating the statutes as per the changing times and needs.

Keywords: Artificial Intelligence, Right to Privacy, Social Divide, India, Data Protection Laws, Digital Divide



INTRODUCTION

India is encouraging AI expansion on a large scale, but policies and legal safeguards built in this context are developing much more slowly, it is observed that India might already be experiencing silent data leakages into Artificial Intelligence systems because regulatory frameworks are evolving comparatively very slowly and enforcement of policies and laws made in the field remains limited. AI growth in India should not come at the cost of its citizens' privacy (Kapoor, 2025). Artificial Intelligence systems use datasets containing personal details of individuals such as browsing history and improper management of this data can potentially lead to privacy violations. Current times are times of AI power, but they should be times of AI privacy. AI privacy refers to safeguarding every individual's personal and sensitive information used by such systems, such as many users are in the dark about their information being used to train AI models. Their data can be misused for profiling, targeted advertising, or manipulation that is why it is very important to balance such high-tech innovations with individual user's privacy protection (Jonker, 2026). The fundamental objective of this research is to examine the negative impact AI has on privacy in India and whether that impact varies across social groups based on education, age, occupation, etc.

India's rapid AI expansion is powered by a growing surveillance economy, where companies continuously collect and use personal data for profit. This began in India in 2017, when start-ups explored using unusual data, such as mobile recharge history, spending behaviour, etc. It is profoundly concerning that even AI developers often cannot fully predict future AI behaviour; data collected by AI systems appearing to be harmless can be used to make sensitive conclusions. For example, repeated small payments could be a sign of cigarette purchases; our personal behaviour is becoming a commercial product in this age of surveillance capitalism (Roy, 2026). This reveals the negative impact AI has on privacy in India to a certain extent, and this underscores the need of attention and extensive analysis of this impact across social groups and arenas.

AI has the potential to turn non-personal data into personal information, which enlarges the grip of this New Leviathan making it harder to define and protect personal information, with a blurry definition, under the existing laws related to privacy in India. Traditional approach for privacy protection was applying principles such as data minimisation and informed consent, but these principles are already being compromised into the clutches of machine learning based



AI systems, which run on collection of massive datasets. ([Artificial Intelligence and Privacy – Issues and Challenges, 2017](#)) These systems ask for permission of using individual's personal data, but because the purpose is not clearly known, it undermines meaningful consent; this grip of Artificial Intelligence might be a potential choke of basic privacy principles which traditionally safeguarded individual's data.

2.1 - Legal and Historical Background –

Surveillance in India has its origins in colonial administrative practices such as the census classification and fingerprint biometric identification systems used by the British Raj during the colonial censuses of 1872 to 1881 ([Kalyani, 2026](#)). These systems weren't merely tools of demographic collection but also the structure of the 'divide and rule' with institutionalized classification through religion, caste, and tribe. These mechanisms enabled bureaucratic control over communities in India by making the Indian population 'legible', a concept discussed by *James C. Scott* ([Coyne, 2025](#)).

The persistence of surveillance after independence eventually raises concerns about one's individual liberty and control, leading the constitutional right to privacy to gradually evolve through the judicial interpretation of Article 21, which guarantees the right to personal liberty and life, has been challenged in Indian courts, making landmark cases like *Kharak Singh v. State of Uttar Pradesh* in 1962, which questioned the intrusive police surveillance practices and unlawful domiciliary visits ([Kapoor, 2024](#)).

It became fundamental after Justice *K.S. Puttaswamy & Anr. vs. In the Union of India*, government surveillance was challenged on the grounds that it violated the right to privacy, which is a constitutionally protected right and is essential to human dignity, autonomy, and liberty ([Garg, 2022](#)).

In 2018, upholding the validity of Aadhaar-UIDAI, launched in 2009, the court under the (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, found it a legitimate state measure to prevent leakage in welfare schemes, but ruled out it as a violation of the right to privacy to make it mandatory in private services like mobile connections, bank accounts, etc ([Aadhaar Act, 2016, 2026](#)). The court established that the right is not absolute. Any infringement by the state must satisfy the "Principle of Proportionality," meaning it must serve a legitimate state aim, be backed by law, and be proportionate to the objective ([Observer, 2023](#)). Today, Aadhaar identifies over 99.9% of India's adult population, backed by section 69 of the IT Act ([A UNIQUE IDENTITY FOR THE PEOPLE, 2022](#)).



Contemporary AI-driven governance similarly depends upon large-scale categorization, profiling, and data extraction. With growing AI surveillance, consent is being questioned at airports, apps, and areas of facial recognition. With only 37% of digital literacy in India, (Sri, 2026) AI systems may deepen existing inequalities through biased datasets, risk of misidentification, particularly among marginalized and rural communities with limited access to legal remedies.

India's shift from colonial models of classification and surveillance systems to modern AI-driven governance thus reflects the emergence of a powerful data-centric state where efficiency, welfare, and national security increasingly rely on large-scale data extraction and algorithmic monitoring. While constitutional protections such as the right to privacy and the Digital Personal Data Protection Act, 2023, attempt to safeguard individual autonomy and informational dignity, (Parliament, 2023) the rapid expansion of AI continues to raise critical concerns regarding surveillance, consent, algorithmic bias, and the widening of existing social inequalities in India.

Certain critical factors that shape young users' positive perception of AI privacy are that young users are expecting clear, accessible, and detailed information about how their data is collected, used, and protected. Trust of youngsters depends on transparent communication about data practices from these systems and adherence to ethical standards such as accountability. Interestingly trust is also shaped by social validation through peer endorsements, user-friendly interfaces can also increase trust of people, also regular updates given about data policies and privacy features of such systems can help in maintaining a trust-based relationship with users (Shrestha, 2024). Privacy fatigue also contributes to this trust and social validation.

This evolving discussion has traced evolution of privacy laws in India and has also highlighted constitutional status of the right to privacy in India, also discussed how despite awareness of hindrance in privacy there is trust built on AI tools because of social validation and privacy fatigue. An overview of legal background is necessary but it cannot fully address or evaluate the complexities of relationship between AI, privacy and social divides. It becomes necessary to explore and engage with scholarly opinions on the intersections and depths of these major aspects of this research. A review of AI driven privacy challenges in modern era is important to identify the existing research gaps in this field.



THEORETICAL FRAMEWORK AND LITERATURE REVIEW

This literature review explores the inter-relationship of Artificial Intelligence (AI), right to privacy and social divide in India and the influence of socio-demographic characteristics on these relationships. In India, these have sparked the debate around AI, privacy and democratic freedom. Concern regarding the rise of technologically empowered states is highlighted in literature, affecting citizens never seen before. (Gilani et al, 2023). This developing structure of power is conceptualized as New Leviathan, where the increasing influence of the government and private companies over public life and information is described.

The concept of Leviathan has come from Thomas Hobbes book *The Leviathan*. Hobbes has justified a strong sovereign authority to maintain social order and security. The current scholars in this digital age re-interpret this concept. And argue that modern states are becoming dependent on surveillance technology like biometric systems, facial recognition and algorithmic governance mechanisms to regulate citizens (Khatun, 2026). Aadhaar-linked authentication, the increased use of facial recognition technology by law enforcement agencies and the rapid spread of CCTV surveillance. These techniques compel people to behave uniformly, not only by coercion but also through the fear of constant surveillance. Therefore, Michael Foucault's theory of disciplinary power and the panoptic on remain a core theory to understand how surveillance works by continuous monitoring and normalisation of behaviour. (Foucault, 1975).

Hobbes theory of sovereignty, Foucault's theory of disciplinary surveillance provides a unique perspective to understand contemporary AI governance. Hobbes helps us to understand how the state justifies surveillance in the name of state security, Foucault explains how citizens are disciplined through continuous surveillance, and hence, these theoretical perspectives provide an analytical framework to understand the evolving surveillance structure of India.

AI's ability to manipulate algorithm is in real time restricting individual's right to non-discrimination by augmenting already existing biases. it is a system which helps in generating deep fakes, which is alarmingly vicious because it can be used as a tool of variety of manipulations; ranging from personal to political; causing serious harm to individual's reputation and violating privacy (Saikia, 2025).



There is an immediate need of well-founded legal guards against new age's digital slavery, for safeguarding privacy of individuals; there is an urgent need of regulations those beyond the conventional directives or laws. This new leviathan and its limbs; specifically, deep fakes, discriminatory algorithms, AI; are threatening to core substances of India; such as democracy, individual liberty and dignity (Tharoor, 2026). AI systems are rapidly used as a tool for spreading misinformation, with these systems foreign actors have an access to personal information of Indian citizens that can potentially weaken democracy in this era of information warfare, which is why it becomes crucial to examine and analyse all limbs of this new leviathan.

There is a need of deeply strengthened national and international coordination to prevent humans from losing control over potentially overpowering and destructive artificial intelligence. This race towards super intelligence in competitive clutches of capitalism has roots in distrust, where AI companies have a desire to take control over the future of this Leviathan. Future potential of AI is a head for recursive self-improvement (RSI) (Ladish, 2026). Major governments of world have to monitor the development of AI in the companies within territory of their geographical boundaries.

The New Leviathan also comes with a great deal of ethical and legal challenges, in a democracy transparency is a vital for legal principles such as accountability, right to information and informed consent, but these AI systems operate in a black box system, and that leads to curtailing of transparency; without transparency it becomes difficult to understand where the border for security is to be drawn to make sure that individual's right to privacy remains protected. (Artificial Intelligence and Privacy – Issues and Challenges, 2017) The gap between multiplying capabilities of such technologies and limited capabilities of existing legal frameworks in India is profoundly concerning for all, the difference between there pace of growth is dangerous, legal ambiguities of scope of data protection laws in the current times is a challenge that demands immediate attention.

Steven Feldstein, in his seminal work "The Global Expansion of AI" has examined the expansion of artificial intelligence worldwide. Out of 176 countries seventy-five are actively using the AI for surveillance motives. This has a huge implication over the governance structures, democratic set up and civil liberties. This Global Expansion of AI reflects the complete dependence of states over AI and the smart monitoring systems. The main argument of Feldstein is that Artificial intelligence (AI) is becoming the key instrument for the states in



terms of governance. AI is enabling the states to strengthen their monitoring systems such as facial recognition and predictive policing. Thus, Feldstein enrap upon global expansion of such technologies and their implications over civil liberties and rights. (Feldstein, 2019). Complementing this broad scale perspective, (Zitek, 2024) scrutinize an individual's psychological response towards AI Surveillance. Their innovative findings illustrate that people grasp AI Surveillance as trespassing human surveillance, which they believe interrupts their autonomy and creates greater resistance towards the monitored environment. Whereas Feldstein mentioned about institutional governance relying over the AI monitored systems, Schuland and Zitek's centre of attention is behavioural and psychological consequences for citizens. Thus, inclusively these studies suggest that the ramifications of AI not only be understood through governance structures but also through its impact on public trust, autonomy and their rights

The above mentioned studies suggest the expansion of AI Surveillance and its implications over the citizen's autonomy and privacy rights. There is another broader political concern about the normalisation of Surveillance associated with digital authoritarianism. This shows it is not just the mere use of technologies but becoming inherent in the governance structure as a tool of repression. Drovic analyses digital authoritarianism in the context of normalisation of Surveillance while doing comparative study of hunger, turkey and India in which he depicts how these hybrid regimes manipulate the legal institutions and electoral processes to perpetuate their authoritarian pattern. This comparative analysis of him highlights that the consequences of digital surveillance are not moulded just by the availability of technological tools but there is a huge influence of political and institutional arrangements under which they are deployed. Thus, the analysis says that AI Surveillance is becoming the tool of power for the states, and therefore this growing capacity of the states to collect, process and monitor the personal information could transform the state- citizen relationship. (Drovic, 2025)

However, the informational power is not just confined to the state but building a state corporate nexus. Dean Curran in article “Surveillance capitalism and systematic digital risks” analyses surveillance capitalism as the new informational surveillance and expands the theory of “Shoshana Zuboff's - the age of surveillance capitalism”. The article evaluates the data extraction from the people and related possible systematic digital risks. Under information capitalism, the dominant business model has been established in the form of the internet and social media. The social media users are neither the customers nor the product, rather their



actions are raw materials that extract the behavioural data, and this helps digitally networked corporations in profit making. Several platforms are being used such as cloud computing and IoT devices. These digital platforms connect them from everyday life aspects, but the same algorithmic failures could lead to socio-economic and political disruptions. Thus, the conditions of systematic digital risks, where the algorithmic failure even at the smallest level could lead to the interdependence over these technologies. This structural dependency is so fragile without adequate alternatives and safeguards (Curran, 2023).

Okonkwo in his article explains the state corporation nexus, where the state deploys surveillance for public order and national security and corporations use it for consumer profiting. To overcome the dilemma, the article suggests, Align AI surveillance with international human rights standards, opting for transparent and accountable mechanisms and advancing global cooperation and harmonisation (Okonkwo, 2023). As a whole Curran and Okonkwo signifies that surveillance in this digital era cannot be acknowledged specifically as a state monitoring practice or profit making module, rather as an intersection of two forms of informational power creating the state-corporate nexus. Hence citizens may counter overlapping forms of surveillance from both public and private institutions and this makes the matter of privacy rights more complex.

Beyond the considerations of privacy matters regarding the AI monitoring systems and surveillance, it is equally significant to scrutinize the socio-economic inequalities that determine the access and experiences of digital technologies. There is a list of factors contributing to the digital inequalities in urban and rural India; to be specific, economic disparities influence the ability to benefit from digital technologies, with the rural economy remaining largely digitally excluded. Socio-economic differences, such as class, caste, and rural-urban divides, are the root causes of digital inequalities. It is notable that the digital ecosystem and access to the internet in rural belts are very poor; there is a lack of basic digital literacy that causes capability inequality and lack of up skilling opportunities in these areas. Societal conditions in these areas are not conducive for maximising digital opportunities effectively, basically limiting the possible benefits of digitalization, and all of these factors create a complex technological social digital divide (Laskar, 2023).

Education and income differences play a critical role in describing the caste-based digital divide in India. There are limited educational opportunities for disadvantaged castes, which



result in lower digital literacy, which augments their digital exclusion. Lower income among disadvantaged caste groups limits their purchasing power, and education is what can enhance their capacity to use digital technologies; other than that, definitely higher income can enhance their access to such technologies (Vaidehi, 2021).

While socio-economic inequalities mould citizens' way to access the digital technologies, the legislative regulatory framework and governance structures are important to determine how these digital technological frameworks should be managed and supervised. Historically, the legal system operated under the Indian Telegraph Act 1885 and the Information Technology Act 2000 provided the initial legal basis for surveillance and data regulation in India, but they are inadequate for addressing the complexities of modern digital technologies. According to Kaur. These laws provide wide powers to conduct surveillance but weak protection of individual privacy, disturbing the balance between state security and fundamental rights. Yet this legal trajectory poses a larger analytical question: why has the Indian state, across democratically elected states with different ideological beliefs, consistently reproduced executive-centric surveillance architecture? This legislative development can be understood as an indication of a deeper institutional tendency to extend the state's capacities in the name of national security, administrative efficiency and digital governance. She is advocating for more judicial oversight, more accountability from judicial bodies, and stronger privacy protections to ensure surveillance is legitimate and in line with the Constitution. (Kaur, 2025).

The Digital Personal Data Protection (DPDP) Act, 2023 has attracted a spectrum of scholarly interpretations at what extent it protects privacy in the rapidly changing digital ecosystem of India. Anita Yadav said the Act signals India's attempt to balance privacy protection and economic growth and digital innovation (rather than the European Union's rights-based approach). They say the DPDP Act is a sign of a pragmatic regulatory mind-set, encouraging cross-border data transfers and bolstering India's digital economy, but also point out that this development-oriented approach offers less privacy protection than the fundamental rights framework of the GDPR (Yadav and Pandey, 2025).

Kumar & Dalal acknowledge the importance of DPDP act but also raises a question that, whether it is sufficient to protect the fundamental rights of the people in the age of artificial intelligence? He argues that broad exemptions provided to the government, limited algorithmic accountability and right to explanation (right to know the reasons for the decision) and



addressing the AI based surveillance and AI based unclear automated decision-making, question the ability of this Act. The authors argue that effective privacy protection requires strong constitutional guarantees, more openness and independent oversight, in addition to traditional data protection laws (Kumar & Dalal, 2025).

Research shows the impact of AI is a double-edged sword for marginalised Indian people, and the effect of this technology is shaped by a range of factors including caste, class, gender and place of birth. Besides this, the government initiatives which include Bharat Net and India AI Mission, and AI tools such as Bhashini, have contributed to providing digital literacy (Nangial, 2025).

But it has some drawbacks besides the positive side. He argues that AI systems often get trained on out dated, biased and old data, which replicates systemic bias; thus, it leads to discriminatory results in social welfare schemes (Dinker, 2024). Deployment of facial recognition technology (FRT) in rural areas often results in over-policing and threat to civic liberty. However, DPDPA 2023 gives a framework for privacy protection, but its broad state exemptions leave marginalised Population continually under surveillance, who lack digital literacy. As a result, instead of working as an independent means, AI can cause more serious damage to the social divide and can automate the traditional exclusion practices (Kaur, 2025).

Thus, all the literature highlights the evolution of AI, how the governance has transformed across the globe, how the power of state and corporations have been strengthened and these developments are giving birth to novel forms of digital inequality and at the same time raising concerns about the right to privacy. The existing literature has broadly examined AI Governance, surveillance capitalism, AI surveillance and the constitutional and regulatory frameworks in India. Very confined research evaluates the public outlook and understanding towards the right to privacy and AI Governance, and the awareness regarding increasing concentration of power in the hands of states. Therefore, there is a need for citizen orientated evaluation of AI privacy, awareness and increasing social divide within the Indian context. Hence, this study investigates the empirical data about the difference of awareness among socio demographic variables and the relationship between the AI awareness, privacy and consciousness.



RESEARCH METHODOLOGY

This research study uses a mixed method that combines qualitative and quantitative research to collect in-depth analysis and perspectives from different individuals affected by AI privacy, digital surveillance, and social demographic disparities. We chose this mixed-method design because it helps us cross-check the data. Quantitative surveys provide measurable trends about privacy awareness. Meanwhile, qualitative open-ended responses give us detailed, lived experiences that numbers alone cannot capture.

4.1. Research Design

This investigation adopts a qualitative exploratory open-ended question designed to collect lived experiences of individuals while using AI in their daily lives. By employing an inductive methodology, the research aims to derive theories and insights from the collected data, rather than only validating pre-existing hypotheses. It also examines quantitative data by using Likert scale to measure the individual's attitudes towards AI impact in their lives.

4.2 Data Collection Methods:

a) Targeted Primary Data Collection (Digital Survey):

The study involved the collection of primary data through a structured online questionnaire which was sent out using Google Forms. The survey was created in order to obtain the public's opinions on AI surveillance, data privacy, and digital exclusion; it contained a combination of closed-ended questions (which were used for mapping out statistical trends) and open-ended questions (in order to pick up the more detailed, qualitative views on the erosion of privacy). We collected data in a month of May 2026, gathering a final sample of over 150 respondents. Participation was entirely voluntary and based on prior consent.

b) Document Analysis:

The primary survey data is aligned by a strict review of secondary literature from the renowned platforms. The study also systematically reviews existing literature, legal frameworks, and policy documents such as International Journal of contemporary research in multidisciplinary, Frontiers of sociology, Indian Journal of Legal Review, AI and Ethics, Legal Issues in the Digital Age, Frontiers in Pharmacology etc. Our study utilizes existing study available online for our research to contextualize & re-evaluating the existing "digital divide," highlighting how



unequal access to AI technologies and educational resources reinforces social demographic stratification. The literature validates along with the minor survey's findings, particularly the respondent's consensus that financial barriers such as the high cost of premium AI subscriptions and advanced hardware such as smart phones create significant obstacles to digital equity.

4.3. Sampling Strategy

The study utilized a convenience and snowball sampling strategy through digital distribution. This method allowed for rapid, cross-regional data collection while ensuring a diverse mix of educational backgrounds (from school-level to doctorate), age cohorts (18–24 and 25–35 age cohorts mainly), rural – urban dichotomy, and financial barriers while accessing AI etc. By capturing responses from individuals actively utilizing social media and digital platforms, the sample accurately reflects the populations most immediately impacted by AI integration and potential data privacy breaches.

4.4. Data Analysis Integration

The survey carried out using Google Forms produced a rich dataset which included both closed-ended metrics and open-ended qualitative narratives. To provide a comprehensive view of the research problem, the quantitative and qualitative findings were directly integrated during the analysis phase. The statistical trends found in the survey data were put into context by referring to the real-life experiences of the respondents who had been obtained from the open-ended replies, so that the qualitative themes could explain the reasons behind the quantitative figures.

a) Hypothesis Testing Techniques:

This research examines Quantitative survey data that will be analysed using statistical software (such as SPSS) beginning with descriptive statistics to summarize the respondents' socio-demographic profiles. To systematically evaluate the research hypotheses, inferential statistical techniques were applied at a standard significance level of 0.05. For the evaluation of the strength and direction of monotonic relationships between ordinal variables, i.e., the correlation between the levels of AI awareness and the corresponding privacy risk concerns and the correlation between ranked educational attainment and awareness of AI's impact on privacy, Spearman's rank correlation coefficient will be used to test H1 and H2. For the test of H3, the Chi-square test of independence will be used; this non-parametric test is appropriate to determine if statistically significant associations are present between purely categorical socio-



demographic variables (such as age, gender, occupation, area of residence, and language) and the respondents' varying levels of AI awareness and privacy concerns.

Alignment of Hypotheses and Statistical Tests

Hypothesis	Description	Statistical Test
H1	Correlation between individuals' understanding of AI and their subsequent awareness regarding privacy risks.	Spearman Rank Correlation
H2	Association between ranked educational qualifications and awareness of AI's impact on privacy.	Spearman Rank Correlation
H3	Significant differences in AI awareness, privacy rights, and privacy concerns across categorical socio-demographic variables.	Chi-Square Test of Independence

b) Thematic Extraction:

The open ended responses underwent a manual thematic analysis to find significant concepts associated with social divides. We used MS Excel for the coding process to ensure a detailed understanding of the respondents' context. The process started with a careful review of the raw text to create initial qualitative codes. We then grouped these codes systematically to find recurring main themes in our study. These themes include Data Colonization, Algorithmic Bias, Privacy Erosion, and Data Protection Laws in India. At the same time, we analysed closed-ended survey responses using SPSS only for descriptive statistics. This helped us identify broader trends in privacy awareness and access to technology, which complemented the qualitative themes we extracted.

c) Real-World Application:

Our Google Forms data revealed respondent real world narratives detailing unauthorized data tracking, targeted advertising, and exposure to deep fake scams were coded under "Algorithmic



Bias and Ethical Concerns." Similarly, consistent mentions of subscription pay walls were coded under "Economic Exclusion," directly reflecting our literature's warning that technological progress can centralize power and resources, leaving marginalized individuals at a disadvantage.

4.5. Ethical Considerations

In the view of the sensitive nature of topics surrounding income inequality, data privacy, and social-demographic divide, this research strictly adhered to ethical data collection standards. Obtaining informed consent was compulsory, with participants receiving detailed information about our study, its aims, and potential consequences before their involvement. Respondent anonymity was prioritised, and all personal information & identifiers were removed from the raw dataset to ensure participants could speak freely about their financial constraints and privacy anxieties without fear of exposure.

RESULTS AND DISCUSSION

This section of the research paper is divided into two parts. The first part will consist of the hypothesis testing and the outcome generated from it and the second part would contain the results and subsequent discussion on the questions that were asked as a part of our research methodology.

Standard deviation measures the spread out of our responses from the average point. low standard deviation indicates high consistency while a high standard deviation indicates low consistency or more scattering of responses.

HYPOTHESIS TESTING:

- i. **Hypothesis (H₁):** Individuals with more awareness/understanding of AI are more concerned about privacy risks

A total of 2 variable types were used, both 5-point Likert scales.

Method of hypothesis testing: The statistical method used to test it was Spearman Rank Correlation.

Table 1: Descriptive Statistics

Variable	Mean	Std. Deviation	Minimum	Maximum
----------	------	----------------	---------	---------



Privacy Concern	4.678	0.615	1	5
AI Understanding	3.592	0.775	2	5

Interpreting the mean value:

Privacy concern had a mean of 4.678 than AI Understands which is 3.592. This means that people have substantially higher concern about privacy whether or not they have the understanding of AI.

Table 2: Correlation Results

Test	Correlation Co-efficient	p-value
Spearman Rank Correlation	0.038	0.643

Interpreting the p-value:

This implies that since the p-value is greater than 0.05, hence there is weak correlation between AI understanding and subsequent awareness about privacy. It is not statistically significant.

Hence, Hypothesis is rejected based on the findings.

ii. Hypothesis (H₂): Better education is associated with better awareness of AI's impact on privacy.

Method of the testing: Spearman Rank Correlation was used.

Table 3: Descriptive Statistics

Variable	Mean	Std. Deviation	Minimum	Maximum
Educational Qualification	2.57	0.573	1.0	4.0
AI Privacy Threat Awareness	4.228	0.736	1.0	5.0

Interpreting the mean value:

The mean value of people having AI Privacy Threat Awareness is slightly more (4.228) than adequate educational qualification (2.57). This means that even without sufficient educational qualification, people are aware of the threats that AI brings with it.



Table 4: Spearman's Rank Correlation Results

Test	Correlation Coefficient	p-value
Spearman Rank Correlation	-0.067	0.42

Interpreting the p-value:

This implies that since the p-value is greater than 0.05, hence there is weak correlation between understanding of AI's threat to privacy and educational qualification.

Herein, a correlation coefficient is a statistical measure that calculates the strength and direction of the linear relationship between two variables. The coefficient -0.067 indicates a weak negative relationship.

Hence, the hypothesis is not statistically significant.

iii. Hypothesis (H₃): There is a significant difference in awareness of AI, privacy rights and privacy concerns in India across socio-demographic variables.

Method of the testing: The Chi-Square Test of Independence was used.

Table 5: Chi-square Test Result

Socio-Demographic Variable	Dependent Variable	Chi-Square value	Degree of Freedom	p-value	Result
Age Group	Legal Status to Right to Privacy	11.316	12	0.5021	Not Significant
Age Group	Privacy Concern Level	3.652	12	0.9889	Not Significant
Age Group	Understanding of AI	21.381	12	0.0451	Significant
Age Group	Language barriers in understanding AI Privacy	15.092	1616	0.5179	Not Significant
Age Group	AI Threat to Privacy	53.77	3	0.0	Significant



Gender	Legal Status to Right to Privacy	6.795	3	0.0787	Not Significant
Gender	Privacy Concern Level	0.694	3	0.8746	Not Significant
Gender	Understanding of AI	7.996	3	0.0461	Significant
Gender	Language barriers in understanding AI Privacy	5.727	4	0.2204	Not Significant
Gender	AI Threat to Privacy	2.527	4	0.6398	Not Significant
Educational Qualification	Legal Status to Right to Privacy	13.696	9	0.1336	Not Significant
Educational Qualification	Privacy Concern Level	7.942	9	0.54	Not Significant
Educational Qualification	Understanding of AI	10.424	9	0.3173	Not Significant
Educational Qualification	Language barriers in understanding AI Privacy	8.957	12	0.7066	Not Significant
Educational Qualification	AI Threat to Privacy	9.214	12	0.6845	Not Significant
Occupation	Legal Status to Right to Privacy	21.553	12	0.0411	Significant
Occupation	Privacy Concern Level	18.956	12	0.6412	Not Significant
Occupation	Understanding of AI	12.022	12	0.04280.2709	Significant



Occupation	Language barriers in understanding AI Privacy	7.653	16	0.27090.7425	Not Significant
Occupation	AI Threat to Privacy	9.152	16	0.74250.2646	Not Significant
Area of Residence	Legal Status to Right to Privacy	10.993	6	0.26460.0886	Not Significant
Area of Residence	Privacy Concern Level	11.78	6	0.1652	Not Significant
Area of Residence	Understanding of AI	4.708	6	0.0886	Not Significant
Area of Residence	Language barriers in understanding AI Privacy		8	0.1613	Not Significant
Area of Residence	AI Threat to Privacy		8	0.7883	Not Significant

Herein, Significant means the results are highly unlikely to occur by random chances and rather show a true measurable effect. On the other hand, not significant means that results can be explained by normal random variation.

RESULTS AND DISCUSSION OF THE QUESTIONNAIRE:

The research was conducted through a mixture of qualitative and quantitative methods. A total of 29 questions were asked across a sample size of 150-plus responses. The questions asked were a mixture of close-ended and opened-ended ones, so that our research paper has a more diverse viewpoint. Since the fundamental nature of the research paper was to study the impact of AI in different sections and areas of India, the sample size was methodically taken across different age groups, professions, as well as different parts of the country. Broadly, the results were analysed as such:



a. Do you believe that an individual's income impacts their knowledge and accessibility towards the required knowledge about AI tools?

Most of the respondents answered affirmatively. The respondents believe that people with higher income often have better internet access, devices and educational resources. Better income also helps individuals in getting the proper knowledge to operate the AI tools and use it to one's required expertise

b. What do you think is the legal status of the right to Privacy in India?

While a positive number of people answered it as a fundamental right, the rest were either unsure or claimed it as statutory law.

In 2017, the Supreme Court declared Privacy as a fundamental right under Article 21 in K.S. Puttaswamy v. Union of India. It is very important to understand one's fundamental rights, especially when they are concerned with one's safety and privacy. AI today transcends and penetrates some of our most personal information. Hence, it is important to know that not every data or every movement of oneself is for the government or agency to analyse and track.

c. Where have you encountered the highest explicit prevalence of using AI using the data?

A lot of respondents agreed that social media is the most vulnerable site wherein there are multiple instances of AI usage, whether in reels, messenger or even the photo filters that are newly introduced. The second highest option is Education. We see the government promoting AI usage in education like various chat bots for doubt clearance, Mission DIKSHA which also promotes AI in providing e-content for teachers and students. Other responses are scattered between online shopping platforms, workplace and government services.

In today's time, AI has become an important tool in many fields. It has specially made its use prevalent in social media sites like WhatsApp, Snapchat, Instagram and so on. While it has immensely helped in better facilitation of the apps and the services that it provides, AI has also come under great scrutiny for some of its misuses. For instance, in 2026, the AI chat bot on the platform X, called Grok was reported to create non-consensual sexualized content which the Indian government later put a cautionary warning to it. (['Times of India', 2026](#))

d. Do you read privacy policies before accepting them?

Only a merger of 21% respondents clicked on Always. The others either stated that they sometimes read the policies (47 %- which is the highest with purple shade) and they do not at all (7 %- indicated through red shade).

It is a very concerning response as many times, the privacy policies are ignored in haste, and we tend to accept or allow the government or the private agencies to use or be a witness to

some of our very personal data. Reading the privacy policy helps us to protect our data, be aware of what the concerned website is asking from us and be vigilant towards our safety. On the other hand, when asked if the respondents take steps to protect their data online, most of the responses were either sometimes or always. Therefore, it is important to understand that reading the privacy policy before agreeing is also a major step towards protecting one's data.

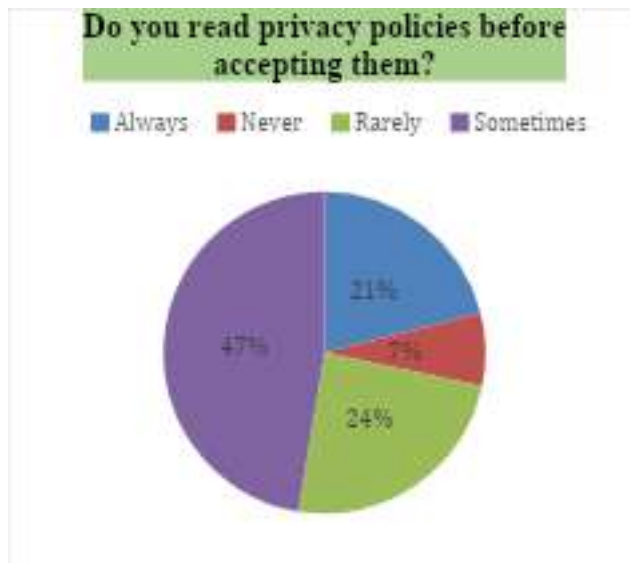


Figure 1

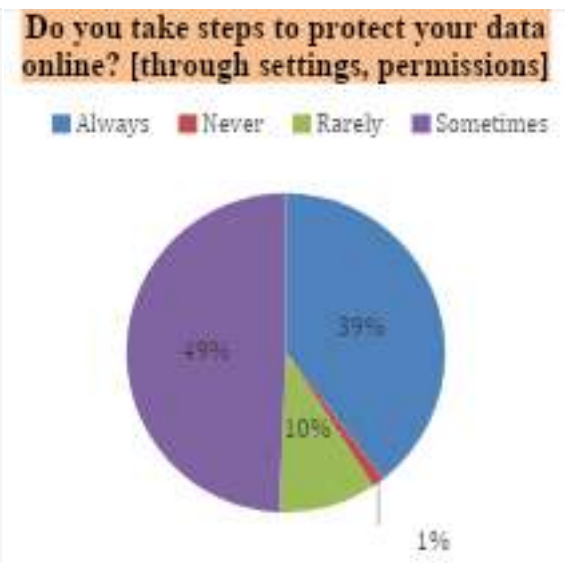


Figure 1.1

Figure 1. It explains the percentage distribution of people who read privacy policies before accepting them.

Figure 2: Explains the percentage of the people who either take steps to protect their data online or they do not.

e. In your opinion, who should be most responsible for protecting user data?

The respondents were given options of government, individuals themselves, private companies, international forums or all the above.

A whole lot of 64% of respondents believe that protecting one's data is a cumulative effort of everyone mentioned in the list. The next highest is Government at 14%, followed by private companies at 9 % and the least is international forums at 1%. As much as we often blame the government or private institutions for infringing their way through our personal data, it is also our responsibility to make sure that we're alert and aware of what websites or online links we are accessing and how much we are consciously and unconsciously giving away our data. An

informed individual, who has knowledge about their rights and digital access, is always at a better foot to secure them.

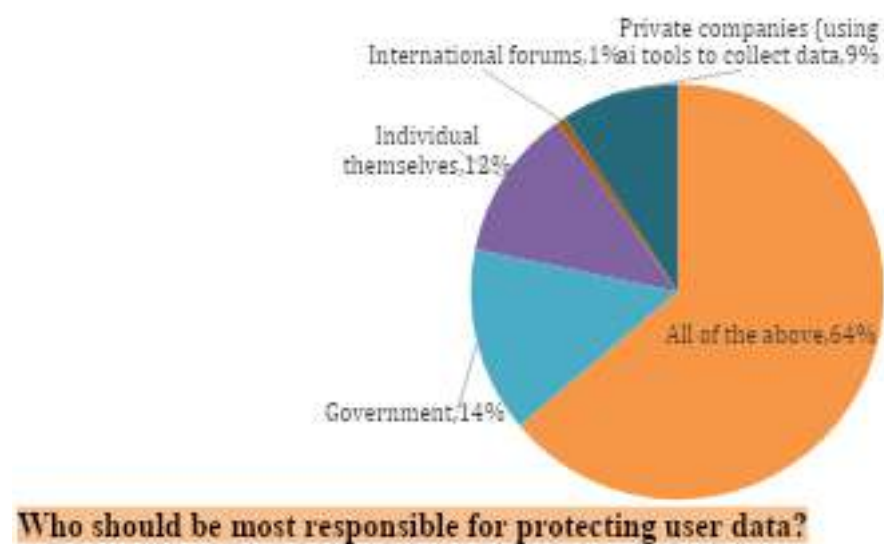


Figure 1.3

Figure 3. It studies the percentage of people's opinion about who is responsible for protecting a user's data.

f. What do you think is one of the prime reasons why India faces disparity in terms of AI knowledge?

For the above question, the respondents were given 5 options: lack of awareness and poor education; lack of interest among sections of society; digital gap between age groups; lack of targeted government policies; lack of regional/area accessibility.

Around 65% people agreed that education plays a very important role in the spread and awareness of AI usage in the world. The second most preferred option was the digital gap between groups which was 16%. The least was lack of regional/area accessibilities at 1%. The research paper mentions in several instances that education plays a very important role when it comes to AI. Since it is a developing concept globally and we are exposed to its newer aspects almost every other day, a proper knowledge and importance about the topic is very essential. Secondly, lack of education is also one of the factors behind the digital gap among different sections and age groups in India. Non-uniformity in terms of digital access, willingness to learn and lack of using digital tools makes it difficult to place all the sections of a society on the same footing when it comes to AI knowledge.

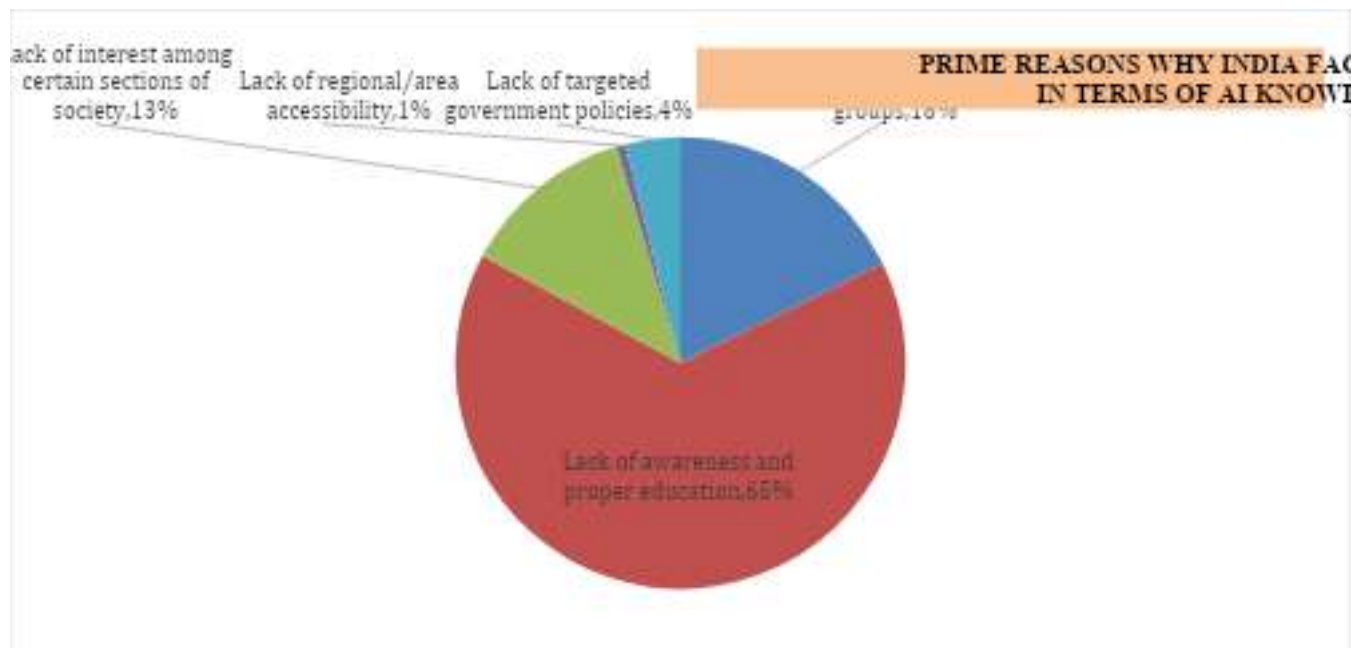


Figure 1.4

Figure 4. It analyses the prime reason why India faces disparities in terms of AI Knowledge.

POLICY IMPLICATIONS

The fast-paced and substantial development of AI in India has presented a critical governance issue for the policy makers. Not only has it highlighted the weak policy structure but also the inefficiency to protect citizen's personal data. India needs robust policy making and immediate action to prevent the rise of "New Leviathan".

- Robust Regulatory Framework for Surveillance Capitalism:** The momentous growth of AI in India has transformed lives but it also outpaces the legal framework by knavishly leaking the personal data of its people. (Kapoor, 2025) The Digital Personal Data Protection (DPDP) Act, 2023 ensures that Indians are given information on where and how their personal data is being used. However, the implementation of the above said act remains weak and more updated rules need to be added to protect people's data. (Gupta, 2026)
- Proper Enforcement of RRI AREA Framework:** Rapidly growing AI sector needs the collaboration of Government and Private sectors over Responsible Research and Innovation (RRI) Area framework.

The framework urges the sector to focus on: (Bhalla, 2023)



- i. Anticipate: identifying the possible risks like data leaks and exploitation of users.
 - ii. Reflect: to examine whether the AI system has any prior biases.
 - iii. Engage: to include peoples from all walks of life to engage over discussion on AI systems
 - iv. Act: making action-oriented decisions to build robust and ethical digital infrastructure.
- **Understanding the Socio-Economics Dynamics:** India is highly diverse when it comes to socio-economic factors. People are divided based on caste, class, literacy, income, social status, rural or urban population. (Laskar, 2023) Marginalized areas and its people lack proper awareness over AI systems and digital infrastructure. Therefore, it becomes important for the policy makers to spread awareness among such people to educate them on personal data protection and digital inclusion. (Vaidehi, 2021)
 - **Regular Policy Updates:** When it comes to the digital world, it has become really difficult to filter out explicit content. It becomes crucial for the policy makers to ensure that the data is provided to the user in a friendly, trusted and transparent source. For this, regular policy updates are needed to make sure user's data is safe and protected.

It becomes important in today's day and age that the conceptual framework and statistical data is correlated to create strong digital infrastructure.

LIMITATION OF THE STUDY

While this paper analyses the AI system in India, potential risks it possesses, digital divide, socio-economic implications and offers critical insights over these areas. However, there are certain limitations that are associated with it that need to be addressed.

- **Restricted Respondent Base:** Considering that India is a highly diverse country in every aspect, the participant pool was compact. The primary limitation was a narrow sample size wherein a total of 29 questions were asked across a sample size of 150-plus responses. Since this study has limited numbers, it cannot be confidently applied to a large Indian population.
- **Constraints on Correlation-based findings:** The Spearman correlation test has shown weak linkages between H1(understanding AI and privacy concerns) and H2(education and awareness on data privacy). It highlighted the fact that even people with better



understanding of AI and better education do not fully understand the privacy concerns associated with it.

- **Social Desirability Biases:** This study was conducted through self-reported surveys with questionnaires and 5-point scales. Such reports can highlight the biases of people like social desirability biases where a few participants can give biased answers to claim that they understand the AI system better than others while still not paying attention to the protection of their personal data being provided online.
- **Digital Exclusion and Online Sampling Bias:** Since the data collection has been primarily done through online surveys, this study is subjected to digital exclusion. Individuals without proper internet connection, lack of digital awareness or without smart devices has been excluded from this sampling. Therefore, this study does not sufficiently represent the vulnerable and marginalised sections of the society.
- **Cross-Sectional Nature of the Study:** The study highlights that the data collected has been collected at a single point in time. Due to its cross-sectional nature, the study points to static perspectives rather than the long term behavioural or policy shifts.

CONCLUSION

The rapid growth of artificial intelligence in India has created a “New Leviathan,” a digital system driven by widespread surveillance that profits from the constant collection, profiling, and commercialization of personal behavioural data. This study examines the connections between AI-driven data collection, constitutional privacy protections, and existing social divides, while successfully achieving its research objectives.

First, the research examined the impact of artificial intelligence on individual privacy and established how existing AI practices undermine the principles of informed consent and data minimization, thereby posing risks to citizens. Second, the study analysed how AI affects different social groups, highlighting variations based on digital literacy and access. A major finding reveals the contradiction between users’ recognition of the need for collective responsibility in data protection, with 64% believing that governments, private companies, individuals, and international forums should all share responsibility, while only a small proportion consistently read privacy policies or regularly take measures to protect their personal information online. Third, the study identified disparities in AI literacy, with 65% of



respondents considering the lack of awareness and proper education as the primary reason behind India's AI knowledge divide.

The hypothesis testing further provides important insights into public perceptions of AI and privacy. Hypothesis 1, which proposed a meaningful relationship between AI understanding and awareness of privacy risks, was rejected. The Spearman rank correlation produced a p-value of 0.643, indicating no statistically significant association. Hypothesis 2, which suggested a positive relationship between educational qualification and awareness of AI-related privacy risks, was also rejected, as the Spearman correlation produced a p-value of 0.420, showing no statistically significant relationship. Hypothesis 3 was partially supported. The Chi-square test revealed statistically significant associations between age group and AI understanding ($p = 0.0451$), gender and AI understanding ($p = 0.0461$), and occupation with legal awareness of privacy rights ($p = 0.0411$), while the remaining socio-demographic variables did not show statistically significant associations.

These findings suggest that legal developments such as the Justice K.S. Puttaswamy (2017) judgment, which recognised privacy as a fundamental right, and the Digital Personal Data Protection Act, 2023, represent important steps towards privacy protection. However, broad exemptions for state agencies and implementation challenges continue to raise concerns regarding AI-driven surveillance. At a time when citizens remain vulnerable to discriminatory algorithms and increased surveillance through technologies such as facial recognition, adopting the Responsible Research and Innovation (RRI) framework becomes essential. Strengthening accountability, transparency, and community participation in AI governance can help ensure that India's rapid digital transformation remains consistent with democratic values, human rights, and responsible innovation.



REFERENCES

1. (2022). *A Unique Identity for The People*. Retrieved from https://www.uidai.gov.in/images/Aadhaar_Brochure_July_22.pdf
2. *Aadhaar Act, 2016*. (2026, January). Retrieved from Grokipedia: https://grokipedia.com/page/Aadhaar_Act,_2016
3. Ajay Kumar Shrestha, A. B. (2024, October). Navigating AI to Unpack Youth Privacy Concerns: An In-Depth Exploration and Systematic Review. *15th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 116 to 121. Retrieved from <https://doi.org/10.1109/iemcon62851.2024.11093125>
4. Alexandra Jonker, A. G. (2026, February). *Exploring privacy issues in the age of AI*. Retrieved from IBM Think: <https://www.ibm.com/think/insights/ai-privacy>
5. Amit Kapoor, M. S. (2025, December). The illusion of privacy in India's AI boom. *The Economic Times*. Retrieved from <https://economictimes.indiatimes.com/news/company/corporate-trends/the-illusion-of-privacy-in-indias-ai-boom/articleshow/125842310.cms?from=mdr>
6. Ankur Pan Saikia, A. K. (2025, May). Exploring the Impact of AI on Privacy and Ethical Considerations: Analysing the Legal and Regulatory Frameworks. *RT&A*, 134 to 147. Retrieved from https://gnedenko.net/Journal/2025/SI_072025/RTA_SI072025-017_17+8-b3-13-p134.pdf
7. *Artificial Intelligence and Privacy – Issues and Challenges*. (2017, September). Retrieved from Office of the Victorian Information Commissioner: <https://ovic.vic.gov.au/privacy/resources-for-organisations/artificial-intelligence-and-privacy-issues-and-challenges/#introduction>
8. Ashmita Gupta, A. R. (2026). Right to Privacy: an Analysis of the Legal Frameworks in the USA, UK, and India. *Indian Journal of Legal Review*, 6, 184 to 188. Retrieved from <https://doi.org/10.65393/vpob1226>
9. Cheng, P. (2024). Regulating the 'AI Leviathan': A Framework for AI Surveillance Disclosure Reporting. *European Business Law Review*, 35(6), 825-850. doi: <https://doi.org/10.54648/eulr2024044>
10. Christopher J. Coyne, N. G. (2025, July). Ways of seeing the world: Legibility in alternative institutional settings. *European Economic Review*. Retrieved from <https://doi.org/10.1016/j.euroecorev.2025.105116>



11. Coeckelbergh, M. (2022, July). Freedom: Manipulation by AI and Robot Slavery. In *The political philosophy of AI*. Retrieved from <https://coeckelbergh.net/the-political-philosophy-of-ai/>
12. Curran, D. (2023, January). Surveillance capitalism and systemic digital risk: The imperative to collect and connect and the risks of interconnectedness. *Big Data & Society*, 10(1). Retrieved from <https://doi.org/10.1177/20539517231177621>
13. Dinker, N. (2024, Dec). Artificial Intelligence and Inequality: Examining the Social Divides Created by Technological Advancements. *International Journal of Innovations In Science Engineering And Management*, 3(2), 228-236. doi:10.69968/ijisem.2024v3si2228-236
14. Dr. Parineeta Goswami, D. S. (2026). The Dual-Edged Sword of Artificial Intelligence In Commercial Law: Enhancing Access While Guarding Against Bias. *SSRN Electronic Journal*. Retrieved from <https://doi.org/10.2139/ssrn.6258205>
15. Drovic, C. (2025). Surveillance Capitalism and the New Social Order: Rethinking Freedom in the Digital Age. *OTS Canadian Journal*, 4(9). Retrieved from <https://doi.org/10.58840/x1dvay91>
16. Feldstein, S. (2019). *The global expansion of AI surveillance*. Carnegie Endowment for International Peace. Retrieved from https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf
17. Foucault, M. (1975). *Discipline and punish*. Paris: FR, Gallimard.
18. Garg, R. (2022). *Constitutional validity of Aadhar Act in the case of Justice K.S. Puttaswamy (Retd.) and Anr. Vs. Union of India*. Retrieved from iPleaders: <https://blog.ipleaders.in/justice-k-s-puttaswamy-ret-d-and-anr-vs-union-of-india/>
19. Gilani, S. R., Al-Matrooshi, A., & Haroon Khan, M. (2023). Right of Privacy and the Growing Scope of Artificial Intelligence. *Current Trends in Law and Society*, 3(1), 1-11.
20. Hamoud Alhazmi, A. I. (2021). Digital Divide and Social Dilemma of Privacy Preservation. *arXiv (Cornell University)*, 1 to 5. Retrieved from <https://doi.org/10.48550/arXiv.2110.02669>
21. Kalyani, G. (2026, May). 11 | 'Imperial Hygiene' and Defective Bodies: Counting Infirmities in Early Colonial Census (1872-1881). Retrieved from India State Stories: <https://www.indiastatestory.in/post/11-imperial-hygiene-and-defective-bodies-counting-infirmities-in-early-colonial-census-1872-18>



22. Kapoor, V. (2024). *Kharak Singh v. the State of Uttar Pradesh (1962): case analysis*. Retrieved from iPleaders: <https://blog.ipleaders.in/kharak-singh-v-the-state-of-uttar-pradesh-1962-case-analysis/>
23. Katkuri, D. S. (2025). A critical analysis of the digital personal data protection Act, 2023. *International Journal of Law*. Retrieved from <https://www.lawjournals.org/assets/archives/2025/vol11issue10/11235.pdf>
24. Kaur, D. (2024). A Comparative Study of the Evaluation on the Right to Privacy in India and the UK, Their Legal Frameworks and Judicial Interpretation: A Cyber Law Perspective. *International Journal of Legal Science and Innovation*, 6(4), 600 - 628. doi:DOI: <https://doi.org/10.1000/IJLSI.112127>
25. Kaur, K. (2025). Digital Surveillance and Indian Privacy Laws. *LawFoyer International Journal of Doctrinal Legal Research*, 3(1), 61 - 77.
26. Khatun, C. (2026). Digital Leviathan: A Theoretical Critique of Algorithmic Governance and the Crisis of Political Obligation in the Context of India's E-Governance Framework. *international Journal of contemporary research in multidisciplinary*, 5(2), 437-442. doi: <https://doi.org/10.5281/zenodo.19453520>
27. Kumar, A., Priyadarshini, A., & Pallavi. (2024). AI And The Right To Privacy: A Comparative Study of Digital Democracies And Surveillance Status In India And The USA. *International Journal of Innovations In Science Engineering And Management*, 3(2), 274-283. doi:10.69968/ijisem.2024v3si2274-283
28. Kumar, V., & Dalal, M. (2025, JUL-DEC). Constitutional Morality in the Digital Age: AI Surveillance and Privacy Concerns. *Journal of Multidisciplinary Knowledge*, 5(2), 212-220. doi: <https://doi.org/10.36676/jmk.v5.i2.147>
29. Ladish, J. (2026, July). AI expert worries about the risk of humans losing control | Four Corners. (A. N. In-depth, Interviewer) YouTube. Retrieved from <https://www.youtube.com/watch?v=gYORRh377Gw>
30. Laskar, M. H. (2023). Examining the emergence of digital society and the digital divide in India: A comparative evaluation between urban and rural areas. *Frontiers in Sociology*, 8, 1 to 8. Retrieved from <https://doi.org/10.3389/fsoc.2023.1145221>
31. Mettipally Navya Sri, N. (2026). Bridging the digital Divide: An analysis on India's digital initiatives. *International Journal for Research Trends and Innovation*, 11. Retrieved from <https://www.ijrti.org/papers/IJRTI2601056.pdf>



32. Mohapatra, K. K. (2025). Digital authoritarianism in India: surveillance, control, and resistance. *International Journal for Multidisciplinary Research (IJFMR)*, 7(3). Retrieved from <https://www.ijfmr.com/papers/2025/3/48656.pdf>
33. Nangial, R. (2025). Democratizing Artificial Intelligence: Bridging the Digital Divide through Inclusive Machine Learning. In N. Kumar, I. B. Lal, & M. Kumar, *Next-Gen Machine Learning: Algorithms for Adaptive Intelligence* (pp. 128-137).
34. Nitika Bhalla, L. B. (2023, December). Ensuring a 'Responsible' AI future in India: RRI as an approach for identifying the ethical challenges from an Indian perspective. *AI and Ethics*, 4(4), 1409 to 1420. Retrieved from <https://doi.org/10.1007/s43681-023-00370-w>
35. Observer, S. C. (2023, June). *Constitutionality of Aadhaar Act: Judgment Summary - Supreme Court Observer*. Retrieved from Supreme Court Observer: <https://www.scoobserver.in/reports/constitutionality-of-aadhaar-justice-k-s-puttaswamy-union-of-india-judgment-in-plain-english/>
36. Okonkwo, O. A. (2023). Ethical tensions between AI surveillance architectures, human rights preservation, and the universal entitlement to digital privacy and dignity. *Magna Scientia Advanced Research and Reviews*, 9(2), 222-238. Retrieved from <https://doi.org/10.30574/msarr.2023.9.2.0179>
37. P R, B., & O, G. (2025, Dec). AI in Social Divides: Data Policies, Structural. *JOURNAL OF SOCIAL COMPUTING*, 6(4), 300–320. DOI: 10.23919/JSC.2025.0021
38. Parliament. (2023). *The Digital Personal Data Protection Act, 2023*. The Gazette of India Extraordinary. Retrieved from https://prsindia.org/files/bills_acts/bills_parliament/2023/Digital_Personal_Data_Protection_Act,_2023.pdf
39. R Vaidehi, A. B. (2021). Explaining Caste-Based Digital Divide in India. 1 to13. Retrieved from <https://doi.org/10.48550/arXiv.2106.15917>
40. Roy, P. K. (2026, January). Privacy | The dark age of surveillance capitalism. *India Today*. Retrieved from <https://www.indiatoday.in/magazine/future-trends-artificial-intelligence/story/20260126-privacy-the-dark-age-of-surveillance-capitalism-by-prasanto-k-roy-2852954-2026-01-16>
41. Schlund, R., Zitek, E.M. Algorithmic versus human surveillance leads to lower perceptions of autonomy and increased resistance. *Commun Psychol* 2, 53 (2024). <https://doi.org/10.1038/s44271-024-00102-8>



42. Tharoor, S. (2026, June). Opinion | The new digital slavery needs constitutional guardrails. *The Hindu*. Retrieved from <https://www.thehindu.com/opinion/lead/the-new-digital-slavery-needs-constitutional-guardrails/article71158538.ece>
43. Yadav, A., & Pandey, R. (2025, Oct 21). Data Privacy Across Borders: A Comparative Analysis of European Union and Indian Protection Laws. *University of Bologna Law Review*, 10(1), 177-214. doi: <https://doi.org/10.6092/issn.2531-6133/22377>