A STUDY ON PROTECTING PRIVACY AND PERSONAL IDENTITY IN THE AGE OF AI AND DIGITAL SURVEILLANCE

Vasundra D, B.COM LL.B. (Hons.), School of Excellence in Law, TNDALU

Raghavi S, B.COM LL.B. (Hons.), School of Excellence in Law, TNDALU

Sveshta Vadhul, B.COM LL.B. (Hons.), School of Excellence in Law, TNDALU

ABSTRACT

The accelerated progression of AI, big data analytics, and ubiquitous digital surveillance has revolutionised society while bringing challenging deformations with profound implications for human rights, including the rights to privacy and personal identity. In the digital landscape, information is being produced on a massive scale by people in their daily lives, enabling states, corporations and technology systems to monitor, profile, and forecast human activities with unprecedented reliability. While such developments create important efficiencies, they also pose challenges and opportunities in the areas of security and innovation, both of which jeopardise personal autonomy, leave individuals vulnerable to misinformation, and facilitate discrimination in decision-making. Facial recognition, algorithmic profiling, biometric authentication – these technologies have increased anxieties about consent, data ownership and the abuse of personal information.

This paper examines the role of digital surveillance and AI-based identity technologies in the protection of human rights. Between the need for security and the need for individual privacy, a gap is created by the lack of transparency and accountability in algorithmic systems, as well as the absence of regulation on how algorithms are both developed and utilised by companies. This has resulted in discrimination, bias, harm, and violations of the dignity of an individual. With the emergence of deepfakes, identity theft, algorithmically biased decision-making and overreaching, there is an urgent need to establish ethical guidelines and provide legal protections to individuals.

It argues for a human rights-based approach to digital governance focused on transparency, accountability, and informed consent as part of AI use. Increasing data protection laws, algorithmic fairness, oversight and access to information are also vital to keeping privacy and identity in an increasingly connected world. Finally, the paper argues that protecting human rights in the digital age is not a legally binding obligation, but a social imperative that serves to preserve trust, democracy, and dignity.

Keywords: AI-Driven Governance, Data Protection, Algorithmic Bias, Digital Autonomy, Ethical Regulation.

1. INTRODUCTION

The merging of AI along with digital surveillance technologies into regular governance, trade and social life is an indication of one of the most remarkable changes of the twenty-first century. AI tools are increasingly used to gather, process, and understand huge amounts of private data that are created through digital communications, biometric identification, and online activity. As a result, these changes have made public administration, law enforcement, and financial services, as well as national security, remarkably efficient.

On the downside, the technological advances that have happened in privacy and personal identity have also changed the meanings and the limits of the concepts. Surveillance is no longer done intermittently or in a conspicuous manner but rather uninterrupted, automated, and sometimes even unnoticed by the persons under surveillance. The systems powered by AI not only monitor people but also foresee and determine future actions, thus putting into question the classical legal concepts of consent, autonomy, and accountability. The paper will investigate the extent to which such changes have an impact on the already existing balancing act between privacy and personal identity as the most important human rights.

2. STATEMENT OF PROBLEM

The broad acceptance of AI-based digital surveillance has resulted in the massive gathering, profiling, and scrutinising of personal data, in most cases without the user's knowledge or consent and even without transparency. The use of these technologies has been justified in terms of safety, speed, and innovation, but the situation has come to a point where they are actually putting privacy, personal identity, and individual freedom at risk. The current laws are inadequate to control the lack of transparency in algorithms, the issue of accountability, and the misuse of data by both the government and private sectors. This absence of regulation has led to various problems, such as discrimination, identity theft, and the deterioration of human rights, consequently raising serious questions about the actual protection of basic rights in the digital era.

3. REVIEW OF LITERATURE

Samuel D. Warren und Louis D. Brandeis – Right to Privacy[1]: Warren und Brandeis kauften

[1] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, **4 Harvard Law Review** 193 (1890).

das Konzept von Privacy as a right in a Court and declared it to be the individual's 'right to be let alone.' Their paper sets the pedestal for modern privacy law and still is one of the main references when it comes to the discussion of how technological developments impose legal safeguards on personal autonomy and identity.

Daniel J. Solove – Understanding Privacy[2]: Solove does not limit privacy to physical intrusion but rather extends its meaning to include informational harms like data aggregation, profiling, and secondary use. He claims that digital surveillance systems are giving rise to structural and systemic privacy risks which makes the traditional consent-based legal models inadequate in tackling AI-driven data practices.

Michel Foucault – Discipline and Punish: The Birth of the Prison[3]: Foucault's surveillance theory describes how monitoring individuals all the time disciplines them and, through the power asymmetries, alters their behaviours. He talked about panopticism, whose concept is of prime importance to AI monitoring as individuals, through self-control, lose their rights of being and identity sensitivity.

Shoshana Zuboff – The Age of Surveillance Capitalism[4]: Zuboff studies how companies turn surveillance-based business models into money through the use of personal data. She points out that this kind of acts actually change the being human to just data about behaviors which then leads to the rights of individuals becoming less important when commercial data exploitation takes place.

Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)[5]: This historic verdict affirmed privacy as a fundamental right, it pointed out the areas in which the right is applicable, like informational privacy, data protection, and digital freedom, particularly in the age of technology, where the rights of citizens are constantly being violated through AI-based surveillance.

4. RESEARCH GAP

The research concerning privacy and digital surveillance has focused mainly on the legal

[2] Daniel J. Solove, *Understanding Privacy* (Harvard University Press, 2008).
[3] Michel Foucault, *Discipline and Punish: The Birth of the Prison* (Vintage Books, 1977).
[4] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019).
[5] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

recognition of privacy rights or the ethical problems of artificial intelligence systems, taken separately. A few papers have been written on data protection laws and constitutional guarantees, but hardly any discourse is there about the merged effect of AI, powered surveillance and automated decision-making on personal identity and human dignity. Besides, the majority of the works take a purely doctrinal or theoretical stance, without substantial inclusion of empirical evidence relating to public awareness, consent practices, and the experiences of digital surveillance in people's lives. Moreover, there is a significant discrepancy in the extent to which future risks such as algorithmic bias, deepfakes, and identity manipulation are talked about in the context of existing legal norms.

5. OBJECTIVES OF THE STUDY

i. To examine how digital monitoring powered by AI affects identity and privacy.

ii. To analyse how algorithmic profiling and biometric technology affect human rights.

iii. To assess the effectiveness of the current legal and regulatory systems.

iv. To evaluate public attitudes and knowledge about digital surveillance.

v. To provide an AI governance strategy based on human rights.

6. METHODOLOGY

This research uses both doctrinal and non-doctrinal approaches to ensure a thorough analysis. The data has been collected from various sources, including well-known academic journals, magazines, official reports, and reliable online resources. This variety improves the reliability of the findings. To interpret the data effectively, we used statistical tools like the percentage method and the average method. The study is based on a sample of 149 respondents, carefully chosen to reflect relevant perspectives. It has been conducted over five months, allowing enough time for detailed observation and analysis.

7. SIGNIFICANCE OF THE STUDY

This study is important because it discusses how AI-driven digital surveillance is increasingly affecting people's privacy and sense of self from both a personal and governmental standpoint. It strengthens digital autonomy and informed decision-making by raising people's

understanding of data gathering methods, consent, algorithmic bias, and accessible legal protections. From a governmental perspective, the study helps policymakers strike a balance between technology innovation, national security, and human rights commitments by illuminating the flaws in current regulatory frameworks. The study assists in creating ethical regulations and maintaining public confidence in digital systems by advocating for an open and rights-based approach to AI governance.

8. HYPOTHESES OF THE STUDY

H1: Digital surveillance backed by AI seriously compromises human identification and privacy.

H2: Human rights violations resulting from computer algorithms cannot be adequately addressed by current legal frameworks.

9. LIMITATIONS OF THE STUDY

The part of the study that's not about rules and laws is based on a small amount of original information because we did not have a lot of time, we could not get to all the information we needed, and we did not have enough resources. This means that the findings from our research may not be true for everyone and may not cover all the points. Additionally, artificial intelligence and digital surveillance are evolving rapidly, with new technologies being developed constantly, which may impact the relevance of some of the findings we have discovered. Furthermore, the research primarily examines the legal, ethical, and societal implications of AI-driven surveillance, rather than engaging in an in-depth technical or computational analysis of AI system design, algorithmic architecture, or engineering processes. As a result, the study focuses on normative and regulatory concerns rather than technological implementation details.

10. RESULT AND DISCUSSION

PART A- DOCTRINAL RESEARCH

Privacy and Personal Identity as Fundamental Human Rights

The right to privacy and the protection of personal identity are universally acknowledged as

the most important human rights that uphold dignity, independence, and freedom of choice. Article 12 of the Universal Declaration of Human Rights states that civilised people should not be subjected to arbitrary interference with their privacy, family, home, or correspondence.[6] This protection was later fortified by Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which requires States to set up legal measures against unlawful or arbitrary invasions of privacy.[7] The UN Human Rights Committee has asserted that this protection concerns both physical and informational privacy, embracing data processed by both public and private bodies.[8]

Today, the personal identity of a user on the web is greatly dependent on their data profiles, biometric markers, and machine learning-based categorisations. Some posit that the right to informational privacy dominates the right to have an identity as people's digital footprints have been made so large that they directly influence their social and monetary, as well as political, participation.[9] The inability to control one's own data makes one vulnerable, thus compromising the person's dignity and independence.

Digital Surveillance and State Responsibility

The use of artificial intelligence and big data analytics for digital surveillance enables the constant collection, creation, analysis, and forecasting of people's behaviours. Although Governments frequently support the use of surveillance for the purpose of maintaining National Security and Public Order, International Human Rights Law requires that any interference with an individual's right to privacy be based on the principles of legality, necessity, and proportionality.[10] In addition, the UN Special Rapporteur on the Right to Privacy has expressed concern over the impact of mass surveillance systems without transparency and independent oversight on the proper functioning of democratic governance and civil liberties.

If a government does not operate under a legislative framework to monitor and collect information, it could potentially chill or deter an individual from exercising his or her right to free speech, assembly, movement, etc.[11] If there is no clearly defined Legislative framework

[6] Universal Declaration of Human Rights, G.A. Res. 217 (III) A, art. 12 (Dec. 10, 1948).
[7] International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171, art. 17.
[8] U.N. Human Rights Comm., General Comment No. 16: Article 17 (Right to Privacy), ¶¶ 3–4, U.N. Doc. HRI/GEN/1/Rev.9 (Vol. I) (1988).
[9] Daniel J. Solove, A Taxonomy of Privacy, 154 U. PA. L. REV. 477, 488–90 (2006).
[10] David Lyon, Surveillance, Snowden, and Big Data, 1 BIG DATA & SOC'Y 1, 3–6 (2014).
[11] Frank Pasquale, *The Black Box Society* 8–12 (2015).

for accountability of an Algorithmic Surveillance System, there is an increased potential for abuse of Authority and Social Control to occur.

Artificial Intelligence, Algorithms, and Discrimination

There is greater use of AI-based decision-making across many different industries, including policing, welfare distribution, credit scoring, employment screening, border control, etc. The algorithms being used with these AIs are not neutral; in fact, there is research indicating that through the use of biased data and non-transparent algorithms, AI systems can perpetuate existing inequalities and indirectly discriminate against certain populations. Research also shows that due to the lack of transparency, individuals do not have recourse when the decisions made by an AI system affect their rights.

The UN Guiding Principles regarding Business and Human Rights state that Corporations have a responsibility to uphold basic Human Rights, and to refrain from profiting from activities that have a negative effect on others, including through the implementation of discriminatory AI systems.[12] The enforcement of these UN principles is weak and fragmented, meaning that businesses operating in the private industry will likely continue to implement high-risk AI systems with little to no accountability.

Misrepresentation, Deepfakes, and Threats to Identity

The ability for an individual to create high-quality fabricated images, audio, and video of another individual without that individual's consent is creating opportunities for misinformation, harassment and identity-related abuse. Currently, the available legal options to combat deepfakes are scattered and not sufficient to protect against the violations of privacy, dignity and reputation these technologies are creating.[13] Therefore, a coordinated effort must be made to provide legal and ethical protections for individuals affected by the use of deepfake and synthetic media technologies.

Data Protection and Emerging Regulatory Frameworks

Data protection laws are important for protecting people's privacy and identity. In the EU, the General Data Protection Regulation (GDPR) takes a rights-based approach to explain how data

[12] U.N. Guiding Principles on Business and Human Rights, princs. 11–13 (2011).
[13] Danielle Citron & Robert Chesney, Deep Fakes, 107 CALIF. L. REV. 1753 (2019).

will be handled. The GDPR includes consent, purpose limitation, data minimisation and accountability. Article 22 of the GDPR states that no fully Automated Decision Making will occur against an individual that leads to a legal consequence or similar based on an Automated Decision.[14]

Worldwide, ethical governance of Artificial Intelligence has been gaining more focus. The UNESCO Recommendation on the Ethics of Artificial Intelligence outlines the elements of responsible AI, such as transparency, oversight by humans, fairness and respect for the dignity of others. The OECD and World Economic Forum Guidelines include similar principles relating to responsible AI governance and monitoring. However, even with all these guidelines, enforcement remains inconsistent, especially in developing nations.[15]

Need for a Human Rights–Based Digital Governance Framework

The rapid expansion of digital technologies like Artificial Intelligence, big data, and digital surveillance has surpassed the gradual establishment of related legal and regulatory measures, thus putting us at a considerable risk of losing privacy, identity, and eventually, even dignity.[16] International human rights treaties, on the other hand, can be relied upon as a strong basis for safeguarding these rights, yet inconsistencies remain regarding the interpretation of the principles of these treaties, particularly in their implementation in the online and digital world across different countries.

The human rights-based approach to technology mandates that the entire range of digital technologies, particularly AI Surveillance Systems, must comply with basic human rights principles of legality, necessity, proportionality, transparency, and accountability.[17] Any actions infringing on a person's privacy must be conducted according to law and based on a valid reason while being as least intrusive as possible.

As digital governance based on human rights hinges on transparency, people should be aware of how their data is collected, used, and processed, especially in the event of automated decision-making. A lack of transparency or the presence of 'black box' algorithms prevents an

[14] Regulation (EU) 2016/679, General Data Protection Regulation, arts. 5, 6, 22.
[15] OECD, Artificial Intelligence and Privacy, OECD Digital Economy Papers No. 280 (2019).
[16] David Lyon, *Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique*, 1 BIG DATA & SOC'Y 1, 3–6 (2014).
[17] International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171, art. 17.

individual from questioning, contesting and comprehending the results of a decision that infringes upon or limits their rights and freedoms.[18] Thus, an emerging international standard requires AI systems to have the means to explain and audit their decision-making mechanics.

International guidelines, such as UNESCO's Recommendation on the Ethics of Artificial Intelligence and the statements of the Office of the High Commissioner for Human Rights, prioritise human control, fairness, and consideration for human dignity as key factors in the design and use of AI systems. Thus, it is hard to imagine technologies as good or bad; it will depend on how they are used.[19]

A human rights-centred digital governance framework is necessary not just for legal compliance, but also as a means to advance and facilitate democracy and social intercourse. Privacy and personal identity protection in the digital world is of prime importance for public trust, democratic institutions, and technological innovation to be seen as compatible with the values of equality, freedom, and human dignity.[20]

Judicial Approaches to Privacy, Identity, and Digital Surveillance: Comparative Case Law Analysis

Indian Jurisprudence

The landmark judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India firmly established the right to privacy as a fundamental right under Article 21 of the Constitution of India. The Supreme Court acknowledged that privacy includes informational privacy, decisional autonomy, and protection of personal identity in the digital age. The Court specifically warned against unchecked state surveillance and emphasised that any restriction on privacy must satisfy the tests of legality, necessity, and proportionality.[21]

In Anuradha Bhasin v. Union of India, the Supreme Court addressed digital restrictions imposed through internet shutdowns. The Court held that access to the internet is closely linked to freedom of speech and expression and cannot be curtailed indefinitely without procedural

[18] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 8–12 (Harvard Univ. Press 2015).
[19] UNESCO, Recommendation on the Ethics of Artificial Intelligence, ¶¶ 14–24 (Nov. 23, 2021); U.N. High Comm'r for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/48/31 (2021).
[20] Shoshana Zuboff, *The Age of Surveillance Capitalism* 94–100 (PublicAffairs 2019)
[21] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

safeguards. This case is significant in demonstrating how digital control mechanisms can indirectly affect personal liberty and identity.[22]

More recently, in Maneka Gandhi v. Union of India (reinterpretation in digital context), principles of due process, fairness, and reasonableness were reaffirmed as applicable to modern technological governance, including surveillance and data collection practices.[23]

European Union Jurisprudence

In Digital Rights Ireland Ltd v. Minister for Communications, the Court of Justice of the European Union (CJEU) invalidated the Data Retention Directive, holding that mass retention of communications data without adequate safeguards violated Articles 7 and 8 of the EU Charter of Fundamental Rights (respect for private life and protection of personal data). The Court emphasised proportionality and necessity in surveillance measures.[24]

Similarly, Schrems v. Data Protection Commissioner (Schrems I) struck down the EU–US Safe Harbour arrangement for failing to protect EU citizens from intrusive US surveillance practices. This judgment reinforced the notion that personal data protection is inextricably linked to human dignity and identity.[25]

In Schrems II, the CJEU further strengthened data protection standards by invalidating the Privacy Shield framework, stressing that effective judicial remedies are essential to safeguard digital identity.[26]

United States Jurisprudence

Katz v. United States, the Supreme Court established the doctrine of "reasonable expectation of privacy," laying the foundation for privacy protections in surveillance cases. Although pre-digital, this principle remains central to modern data privacy debates.[27]

[22] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 (India).
[23] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248 (India).
[24] *Digital Rights Ireland Ltd v. Minister for Communications*, Joined Cases C-293/12 & C-594/12, EU:C:2014:238 (CJEU).
[25] *Maximillian Schrems v. Data Protection Commissioner*, Case C-362/14, EU:C:2015:650 (CJEU).
[26] *Data Protection Commissioner v. Facebook Ireland Ltd (Schrems II)*, Case C-311/18, EU:C:2020:559 (CJEU).
[27] *Katz v. United States*, 389 U.S. 347 (1967).

Carpenter v. United States, the Court held that accessing historical cell-site location information without a warrant violates the Fourth Amendment. This decision marked a major shift by recognising that digital data can reveal intimate details of personal identity and daily life, warranting heightened constitutional protection.[28]

Riley v. California ruled that police must obtain a warrant before searching digital data on mobile phones, acknowledging the depth of personal information stored digitally.[29]

PART B NON-DOCTRINAL RESEARCH

This brief survey was conducted to collect real-world, non-doctrinal evidence on the level of public knowledge, the common feelings, and the experiences concerning AI, digital surveillance, data protection laws, and human rights issues. Sample size N = 149. The respondent profile leaned heavily towards 'urban' (Urban = 89, 59.7%), while rural consisted of a modest sample (Rural = 23, 15.5%) and Semi-Urban (24.8%). Education skewed degree/PG holders.

TABLE NO.1. Do you believe digital surveillance affects your right to privacy?

Gender	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	Total
Female	31 (20.80%)	20 (13.40%)	15 (10.10%)	0 (0.00%)	0 (0.00%)	66 (44.30%)
Male	46 (30.90%)	27 (18.10%)	10 (6.70%)	0 (0.00%)	0 (0.00%)	83 (55.70%)
Transgender	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)
Total	77 (51.70%)	47 (31.50%)	25 (16.80%)	0 (0.00%)	0 (0.00%)	149 (100%)

Source: Primary data

[28] *Carpenter v. United States*, 138 S. Ct. 2206 (2018).
[29] *Riley v. California*, 573 U.S. 373 (2014).

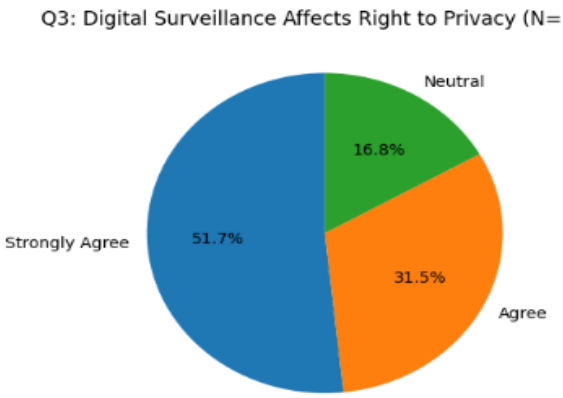


Table No. 1 shows that the majority of respondents tend to believe that digital surveillance affects their right to privacy, with higher male respondents strongly agreeing at 55.7 percentage in total and 30.9 percent strongly agreeing with the statement and 6.7 percentage acting neutral. Female respondents of 44.3 percentage strongly agree with 20.8 percentage and 10.10 percentage being neutral, and Transgender of 0.0 percentage. Distribution by gender indicates that both males and females largely sit on the agree side, and there is 0.0 percentage of disagree, i.e., it is evident that the respondents believe digital surveillance invades everyone's right to privacy.

TABLE NO.2. Are existing data protection laws sufficient to protect privacy and identity?

Gender	Yes	No	Needs improvement	Total
Female	21 (14.10%)	24 (16.10%)	21 (14.10%)	66 (44.30%)
Male	14 (9.40%)	29 (19.50%)	40 (26.80%)	83 (55.70%)
Transgender	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)
Total	35 (23.50%)	53 (35.60%)	61 (40.90%)	149 (100%)

Source: Primary data

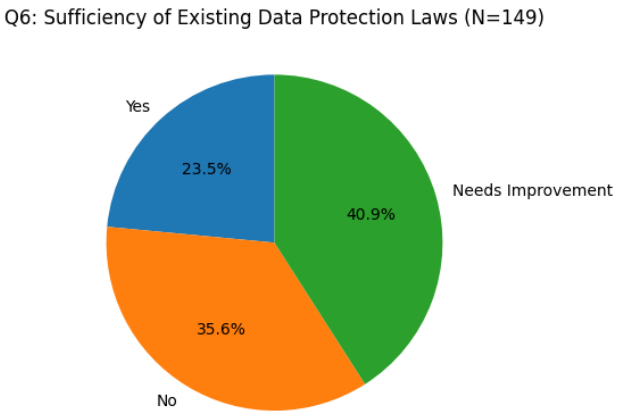


Table No. 2 shows that the respondents accepts that the existing statutory laws on the protection of privacy and identity is not enough, with higher male respondents recommends that the law needs improvement by 26.8 percent and just 9.4 percentage replying yes to the question. Female respondents of 16.10 percentage replied with no, as most of the victims falls in the female group and they aren't aware of such laws, and they seek more protection from these AI digital platforms.

TABLE NO. 3. Do you support a human rights-based approach to AI governance?

Gender	Yes	Maybe	No	Total
Female	42 (28.20%)	17 (11.40%)	7 (4.70%)	66 (44.30%)
Male	57 (38.30%)	18 (12.10%)	8 (5.40%)	83 (55.70%)
Transgender	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)
Total	99 (66.50%)	35 (23.50%)	15 (10.10%)	149 (100%)

Source: Primary data

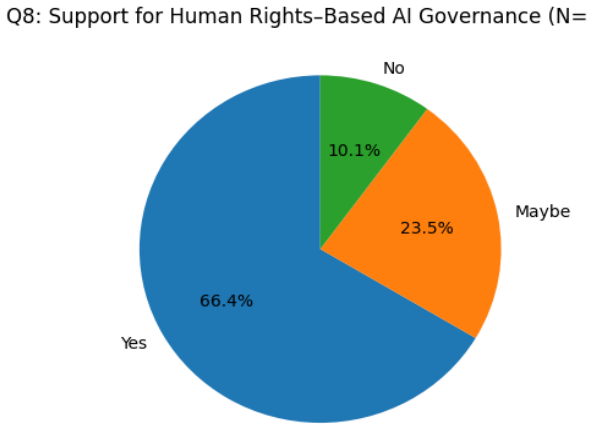


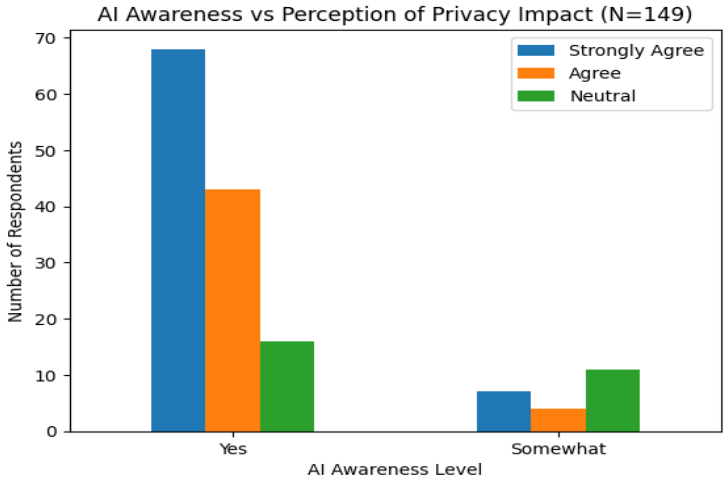
Table No. 3 shows that the majority of respondents supports for human rights-based AI governance. Higher male respondents agreed with 'Yes' at 38.3 percentage in total and 'No' with just 5.40 percent. Female respondents of 28.2 percent supported this governance system with Yes and 4.70 percent replied with 'No', Transgender of 0.0 percentage. This type of mixed answers from the public shows that either the group of people aren't aware of such laws or about the threat of digital surveillance in this digital era

CROSS TABULATION METHOD:

TABLE NO. 4. Awareness of AI × Perception of Privacy Impact

AI Awareness	Strongly Agree	Agree	Neutral	Total
Yes	68 (45.6%)	43 (28.9%)	16 (10.7%)	127 (85.2%)
Somewhat	7 (4.7%)	4 (2.7%)	11 (7.4%)	22 (14.8%)
No	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)
Total	75 (50.3%)	47 (31.6%)	27 (18.1%)	149 (100%)

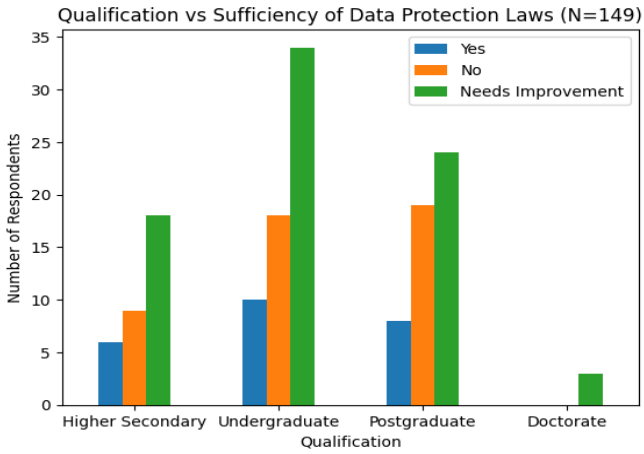
Source: Primary data



The table no. 4 reveals that the majority of those respondents who were very much aware of AI, expressed their strong agreement or agreement with the opinion that the right to privacy is affected by digital surveillance, thus indicating a positive correlation between the awareness of AI and the risk of privacy being perceived. This is a strong backing for Hypothesis H1.

TABLE NO.5. Qualification × Sufficiency of Existing Data Protection Laws

Qualification	Yes	No	Needs Improvement	Total
Higher Secondary	6 (4.0%)	9 (6.0%)	18 (12.1%)	33 (22.1%)
Undergraduate	10 (6.7%)	18 (12.1%)	34 (22.8%)	62 (41.6%)
Postgraduate	8 (5.4%)	19 (12.8%)	24 (16.1%)	51 (34.2%)
Doctorate	0 (0.00%)	0 (0.00%)	3 (2.0%)	3 (2.0%)
Total	24 (16.1%)	46 (30.9%)	79 (53.0%)	149 (100%)



Source: Primary data

From the table no. 5, the results demonstrate that the participants from all educational backgrounds predominantly think that data protection laws should be improved, with dissatisfaction being more pronounced among undergraduate and postgraduate students. This shows a general understanding that the legal systems in place are not sufficient to tackle the issues related to human rights impacted by algorithms, which further substantiates Hypothesis H2.

ALIGNMENT OF EMPIRICAL FINDINGS WITH DPDP ACT, IT ACT & AI ETHICS

1. Alignment with the Digital Personal Data Protection (DPDP) Act, 2023[30]

The DPDP Act, 2023 has declared privacy as a statutory right and managed the digital personal data workflow. Nevertheless, the survey results especially from Question 6 (Sufficiency of Data Protection Laws) indicate that most respondents consider the current laws either inadequate or needing change.

Empirical Alignment: 76.5% of the participants asserted that the existing data protection laws were either not enough or needed to be better. This agrees with criticisms of the DPDP Act regarding:

Limited control of decisions taken by machines, no clear protection against the use of algorithms for profiling people, weak rules on the transparency and understandability of AI

[30] Digital Personal Data Protection Act, No. 22 of 2023, India.

Legal Implications: The results imply that although the DPDP Act is a considerable advancement, it will not fully resolve the issues of AI-based surveillance, algorithmic bias, and personal identity threats. Thus, it implies support for Hypothesis H2.

2. Alignment with the Information Technology Act, 2000

Cyber legislation in India went through the IT Act, 2000 and its rules, which mainly talk about cybercrime and data security measures, and the liability of intermediaries. Still, the act was passed in a time when AI was not in the picture, hence it does not have any specific laws related to AI-powered monitoring systems.[31]

Empirical Alignment: The view of the majority of the people participating in the survey is represented in Question 3's pie chart, where more than 80% (i.e. 83.2%) believe that their right to privacy is impacted by the digital surveillance. The reason for this viewpoint is that the existing laws like Section 43A and the SPDI Rules, are primarily concerned with data security aspects rather than surveillance accountability, thus the perception indicates the inadequacy of these laws.

Legal Implication: The IT Act has no control over the following unlawful activities: Mass digital surveillance, Biometric identification systems, Predictive and automated decision-making by AI. [32]This supports Hypothesis H1, which suggests that AI-based surveillance erodes privacy and personal identity beyond the reach of current IT law protections.

3. Alignment with AI Ethics Principles

The solid empirical evidence for transparency, accountability, and a human rights-based approach to AI governance virtually coincides with the presently accepted AI ethics principles, like: Transparency and Explainability, Accountability, Fairness and Non-Discrimination, Human Oversight, Respect for Human Rights

Empirical Alignment: 66.4% of the individuals polled favour the implementation of a human rights-centric governing approach in AI technology (table no.3). Table no. 4 reveals that more extensive knowledge of AI is connected to higher privacy concerns, which suggests that the

[31] Information Technology Act, No. 21 of 2000, § 43A, India.
[32] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, India.

public is aware of the ethical risks.

Ethical Implication:

The results underscore that:

The application of ethical standards is viewed as necessary in situations where legal solutions are inadequate. Society asks for AI regulations that are based on human rights and dignity rather than just on technological compliance. This argument reinforces that ethical AI principles must further the reach of statutory law in dominant areas like surveillance and identity management.

Testing of hypothesis:

H1: Digital surveillance backed by AI seriously compromises human identification and privacy. From the table no. 1 and 4, there is no notable disagreement among the respondents. This huge consensus shows that the respondents consider digital surveillance as a grave danger to privacy and personal identity. The respondents with knowledge about artificial intelligence (AI) show a much stronger agreement that surveillance has an effect on privacy. The less awareness about AI, the more neutrality is observed. This proves that there is a direct link between the awareness of AI and the concern of privacy. A vast majority of people surveyed strongly agreed or agreed that the privacy impact of digital surveillance and AI awareness has made this perception even stronger; therefore, the thesis is accepted, and it is the null hypothesis.

H2: Human rights violations resulting from computer algorithms cannot be adequately addressed by current legal frameworks. From the table no. 2, a striking 76.5% of the survey participants consider the legislation either to be inadequate or in need of alteration. Just a minority of 23.5% think that current laws are up to the mark. And from the Table no. 3 a vast majority is in favour of the human rights-based approach to AI regulation. This indicates a feeling that the legal protection provided is not enough. From the table no. 5, among people with different educational qualifications, the most common answer is "Needs Improvement". The higher one's educational qualification, the more legal inadequacy one is aware of. Since the majority of the respondents, irrespective of their qualifications, consider the existing legal frameworks to be inadequate and are in favour of a human rights-based AI governance model,

the thesis is accepted, and it is null hypothesis.

11. CONCLUSION

Through a doctrinal and non-doctrinal research approach, the impact of AI and digital surveillance on privacy and personal identity was investigated in this study. The doctrinal research revolves around the fundamental human rights in both India and World nations by highlighting major caselaw judgements and their viewpoints about AI and digital surveillance. The outcomes from the empirical study have shown that the majority of those surveyed believe that AI-based surveillance seriously interferes with the right to privacy and that the current legal systems are not capable of confronting these issues. Besides that, the study points to a great public backing for a transparent, accountable, and human rights-based approach to AI governance.

In summary, the research indicates that on the one hand the DPDP Act and the IT Act can be seen as providing a minimal framework for data protection, on the other they are not enough to face the new threats coming from AI and digital surveillance. Hence, the need for more robust legal protections and ethical government practices that can effectively preserve individuals' privacy and identities in the digital era is very urgent.

Suggestions:

1. Laws should explicitly dictate AI systems that automatically make decisions impacting individuals, and the right to appeal such decisions should be given to people.

2. The transparency of AI systems used for surveillance must be guaranteed and the authorities should inform the public about their methods of personal data collection and usage.

3. Surveillance based on AI technology should be confined to specific situations where it is necessary, and proper legal approval and safeguards should accompany it.

4. Current data protection laws should undergo improvements so that they can effectively deal with the privacy and identity risks associated with AI.

5. The regulation of AI should be grounded in human rights principles such as justice,

accountability, and privacy protection.

6. The implementation of preventive measures against the misuse of biometric and identity-dead data should be done with greater strength.

7. The governments should be at the forefront in making people aware of their digital privacy rights and the risks posed by AI technologies.

REFERENCES

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, **4 Harvard Law Review** 193 (1890).

2. Daniel J. Solove, *Understanding Privacy* (Harvard University Press, 2008).

3. Michel Foucault, *Discipline and Punish: The Birth of the Prison* (Vintage Books, 1977).

4. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019).

5. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

6. Universal Declaration of Human Rights, G.A. Res. 217 (III) A, art. 12 (Dec. 10, 1948).

7. International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171, art. 17.

8. U.N. Human Rights Comm., General Comment No. 16: Article 17 (Right to Privacy), ¶¶ 3–4, U.N. Doc. HRI/GEN/1/Rev.9 (Vol. I) (1988).

9. Daniel J. Solove, A Taxonomy of Privacy, 154 U. PA. L. REV. 477, 488–90 (2006).

10. David Lyon, Surveillance, Snowden, and Big Data, 1 BIG DATA & SOC'Y 1, 3–6 (2014).

11. Frank Pasquale, *The Black Box Society* 8–12 (2015).

12. U.N. Guiding Principles on Business and Human Rights, princs. 11–13 (2011).

13. Danielle Citron & Robert Chesney, Deep Fakes, 107 CALIF. L. REV. 1753 (2019).

14. Regulation (EU) 2016/679, General Data Protection Regulation, arts. 5, 6, 22.

15. OECD, Artificial Intelligence and Privacy, OECD Digital Economy Papers No. 280 (2019).

16. Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 8–12 (Harvard Univ. Press 2015).

17. UNESCO, Recommendation on the Ethics of Artificial Intelligence, ¶¶ 14–24 (Nov. 23, 2021); U.N. High Comm'r for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/48/31 (2021).

18. *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 (India).

19. *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248 (India).

20. *Digital Rights Ireland Ltd v. Minister for Communications*, Joined Cases C-293/12 & C-594/12, EU:C:2014:238 (CJEU).

21. *Maximillian Schrems v. Data Protection Commissioner*, Case C-362/14, EU:C:2015:650 (CJEU).

22. *Data Protection Commissioner v. Facebook Ireland Ltd (Schrems II)*, Case C-311/18, EU:C:2020:559 (CJEU).

23. *Katz v. United States*, 389 U.S. 347 (1967).

24. *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

25. *Riley v. California*, 573 U.S. 373 (2014).

26. Digital Personal Data Protection Act, No. 22 of 2023, India.

27. Information Technology Act, No. 21 of 2000, § 43A, India.

28. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, India.