RECONCEPTUALISING HUMAN RIGHTS IN THE DIGITAL PUBLIC SPHERE: ANALYSIS OF MEDIA, GLOBALISATION, AND EMERGING DIGITAL TECHNOLOGIES (AI)

Diya Patil, BBA LLB, Symbiosis Law School, Nagpur (SIU)

Ria Gulati, BA LLB, Symbiosis Law School, Nagpur (SIU)

ABSTRACT

The technological and digital expansion within the public sphere has witnessed a rapid growth which is shaped by globalization, media convergence, and emerging artificial intelligence technologies. These developments necessitate a fundamental makeover and reconceptualization of the human rights framework. Traditionally ingrained in the state centric sovereignty, the human rights norms are challenged by transnational digital infrastructure that facilitate communication, influence public discourse, and helps in regulating the access to information. Digital platforms are algorithmic which has transformed the nature of participation and has opened and paved the way of surpassing digital ethics by enabling unprecedented connectivity and amplifying the risks of misinformation, data exploitation and algorithmic discrimination.

This research critically examines how media ecosystems and AI driven technologies reshape the ideas of basic human rights such as the right to privacy, freedom of expression, and access to information within the digital public sphere. It proposes the integration of algorithmic transparency, accountability and digital equity within the existing legal frameworks worldwide to ensure protection of human rights in the increasingly mediated world and future of the rights in such a networked society.

Keywords: Digital public sphere, Globalization and media, AI Driven technologies, Digital ethics, Human rights (privacy, transparency, accountability).

1. INTRODUCTION

The modern 21st-century public is no longer confined to streets, town halls and newspapers; it has been migrated, in very large part, to the space of the digital public, an online environment that allows individuals, communities and states to communicate and interact through social media, web based search engines, messaging apps and, increasingly, through the mediation of artificial intelligence (AI) systems which mediate and determine multi-lateral communication and interaction. This cyberspace has altered how basic human rights are exercised, enjoyed and violated creating new doctrinal problems in the constitutional and international law. Formulated in a state-based, territorially defined, world, traditional doctrines of human rights now face transnational data streams, privately directed platforms, and opaque, algorithmic systems of decision-making, the logic of which many defies traditional doctrines of law.

The digital technologies have distorted the classical categories of human rights in digitally mediated versions. The freedom of expression, which previously related to the concept of the press and demonstrations, is now inclusive of the internet speech, algorithmic self-promotion, and autonomous content retrieval. The right to privacy, which is about the protection against unreasonable governmental surveillance, now has to deny the data-gathering efforts by companies, psychographic profiling, and facial-recognition systems unleashed by the state and non-state actors. The equality and non-discrimination right are also being violated in new ways via algorithmic bias, with predictive policing, automated hiring, and credit-scoring devices that run on AI having the potential to cement preexisting patterns of social inequality under the guise of an unbiased data analysis.

Simultaneously, media and globalisation have strengthened the magnitude and the intricacy of these changes. Global media chains and internet space provide people with the ability to take part in transnational popular discourses and to hold states responsive to online mobilisation, whereas it also opens the user to post-national surveillance systems, data-harvesting, and the disinformation complex. The mediatization of international law and globalisation of media imply that the digital space is both an enabler and a threat to human rights and increases participation in democracy and, at the same time, manipulation, polarization, and repression.

The constitutional jurisprudence in India has started to take note of some of these challenges.

Influential cases like Justice K.S. Puttaswamy v Union of India[1] acknowledge the privacy as inherent under the Article 21, including informational privacy, and provide restrictions of the governmental surveillance and bio-metric control. In Union of India vs Shreya Singhal v Union of India[2], the chilling nature of Section 66A of the Information Technology Act was declared unconstitutional and invalid because it was unsuitable in the digital era (in respect of the industry), and the significance of ensuring that intermediary-liability rules are clearly, proportionately, and non-vaguely expressed. The case of Anuradha Bhasin v Union of India[3] stated that the right to the internet is part and parcel of the exercise of 19(1) (a) since digital connectivity is a facilitating right in the modern world. However these innovations have still been construed by Indian courts primarily by analog constitutional reasoning without an entirely spelled out system of AI-specific protections, such as algorithmic transparency, an entitlement to explanation, and automated discrimination protection.

Similar tensions can then be seen internationally. The digital rights can be guided by such normative resources as the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), or regional systems like the General Data Protection Regulation (GDPR), although it is currently biased and inconsistent in applying these guidelines to AI-based systems. The Cambridge Analytica data scandal, which involved gathering personal data of millions of users of social-media platforms to do political microtargeting, demonstrated the ineffectiveness of the current regulatory and doctrine instruments to deal with macro, cross-border, data mining. Cases like Google Spain v AEPD[4], which established a de-linking right of personal data in search-engine results which is analogous to a right to be forgotten, demonstrate that the courts are starting to redefine the privacy and expression norms to the algorithmic intermediaries, but they also indicate the conflict between individual control and freedom of information. State v Loomis in the criminal-justice setting showed the dangers of algorithmic sentencing, where risk-assessment tools are unknown and hidden, and no one has significant insight into how they are applied or their ability to explain the severity of punishment.

This question is posed concerning four overall questions:

[1] (2017) 10 SCC 1
[2] (2015) 5 SCC 1
[3] (2020) 3 SCC 637
[4] Case C-131/12, [2014] ECLI:EU:C:2014:317

What impacts do the shift of the traditional public sphere toward a digital one, characterized by social media and algorithmic recommendation platforms, have on the practice of the freedom of expression, privacy, equality, and democratic participation?

Is it possible that the current human rights doctrine, especially constitutional and internationallaw doctrines are sufficient to control AI systems and platform governance, or are material doctrinal innovations (e.g., new rights, new procedural protection, new horizontal responsibilities in the ownership of the individual actors) necessary?

In what ways does Indian constitutional jurisprudence have doctrinal vacuities with international norms of AI governance (e.g. GDPR style frameworks and the EU AI Act style framework) particularly regarding data protection, algorithmic transparency and accountability?

Are new, explicitly digital human rights such as right to algorithmic transparency, right to explanation, and right to protection against automated discrimination to be recognised and, in that case, how can they be established on the base of current constitutional and internationallaw principles in such a way as to do not weaken the doctrinal coherence?

The methodological concept embraced by the project can be characterized as doctrinal, given that it depends on a detailed study of provisions regarding constitutionality, statutes, treaties, the case law, and academic texts. It will make comparisons with other international and regional human-rights models on one hand and Indian constitutional jurisprudence on the other hand, observing the way in which the court and standard-setter are interpreting privacy, expression, equality, and due process on the internet. Based on theoretical literature addressing the digital public sphere, platform constitutionalism, and algorithmic governance, the project will transition to the critical examination, thereby uncovering doctrinal tensions, inconsistencies and gaps.

2. OBJECTIVES OF THE STUDY

The primary aim of the proposed doctrinal research is to review the reconstruction of human rights in the digital public sphere through the process of media, globalisation, and new digital technologies, in particular, artificial intelligence (AI). The objective of the study is the following:

To examine the ways in which the conventional human-rights principles of privacy, freedom of expression, equality and due process are being revolutionized in digital spaces.

To make comparative assessments of the jurisprudence of the Indian constitution and the pertinent foreign instruments on human rights and AI-governance.

To determine what effects AI, media platforms, and global data flows, as well as algorithmic governance will have on the basics of rights.

To determine loopholes in the current laws and regulations of digital rights.

To suggest a reformulated set of digital human-rights standards which may be incorporated using available constitutional and international-law principles.

3. RESEARCH METHODOLOGY

This research adopts a doctrinal methodology by focusing on the systematic analysis along with synthesizing legal principles, precedents and statutes relating to human rights in the digital age. It analyses how traditional human rights doctrines apply to the digital environment shaped by AI and digital media by means of globalization. It evaluates the evolving jurisprudence concerning the ideas of privacy, free speech, data protection and digital constitutionalism analysing protocols and guidelines laid down globally. This doctrinal research aims to identify the lacunae with the human rights framework in the digital public sphere, proposing normative legal framework, and striking a coherent approach between human rights and the usage of the digitally mediated world.

4. ANALYSIS

4.1 Legal Framework (National and International).

4.1.1. On the International level the initial instruments on human-rights protection are the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and the International Covenant on Economic, Social and Cultural Rights (ICESCR). Despite having been written prior to the advent of AI and mass digitalisation, these instruments are open-textured enough in their wording to accommodate claims of the digital age.

The Article 19 ICCPR (freedom of expression) and Article 17 ICCPR (privacy) are becoming standard points of reference in the debate on online speech, mass surveillance and the regimes of data-protection.

Article 26 ICCPR (equality and non-discrimination) is even being interpreted to include that of algorithmic bias, where AI systems extend prior historical discriminations in hiring, policing, and welfare.

There are specific regulatory examples of data-protection rights and transparency and riskbased regulation of AI models in regional laws, like the European Union off the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act proposal, which have shaped the establishment of global norms.

These tools form a constructivist foundation of the argument that digital rights are not wholly new, but a development of the already established human-rights principles that are now modified to the change created by technology.

4.1.2 Indian Constitutional and Statutory Framework.

In India, the basic rights used in the digital public sphere are given the core doctrine under the constitution of India:

Article 14 (Right to Equality): Ensures equal protection of legislations and plays the key role in requiring the challenge of algorithmic discrimination in policing, welfare distribution, and employment.

Article 19(1) (a) (end of speech and expression): is the online speech protection which curbs the overly broad criminal and intermediary-liability laws (e.g. Information Technology Act, 2000, interpreted in terms of Shreya Singhal).

Article 21 (right to life and personal liberty): Has been used to imply a wide restriction on the right in terms of privacy, dignity, informational autonomy, and arbitrarily surveillant those offenders.

Moreover, the Digital Personal Data Protection Act, 2023 (DPDP Act) provides an official framework on data protection, which entails the right to consent, the right to limitation of

purpose, the right to correct, and the right to grievances redress and the Data Protection Board of India, which is established to monitor compliance. Nonetheless, the DPDP Act is data-oriented and is not fully proportional to the concerns regarding AI-related issues of algorithmic bias, explainability, and human control in automated decision-making.

4.2 Relevant Case Laws

4.2.1 Indian Constitutional Jurisprudence.

Union of India v Justice K.S.Puttaswamy (2017).

In the case of Justice K.S. Puttaswamy, (Retd) v Union of India, the Supreme Court identified privacy as a basic right of the Fourth Amendment of Article 21 which encompasses informational privacy and informational self-determination. The Court stressed that privacy is not merely a line of defence against state-like surveillance, but also against information-loving businesses. Theoretically, Puttaswamy is central as it:

- Brings a constitutional ground to the data-protection law (since then echoed in the DPDP Act, 2023).
- Makes the tests of legality, necessity, and proportionality the markers of any state or privately-based data-collection and profiling effort, such as AI-based surveillance.

Shreya Singhal and Union of India (2015).

In the case of Shreya Singhal v Union of India, the Supreme Court declared the Section 66A of the Information Technology Act, 2000 as vagueness and over-broad and had a chilling effect on online speech. The ruling upheld that intermediaries are not liable of user-created content unless specific and narrowly focused and procedurally fair criteria.

The case is interesting since it establishes boundaries to the intermediary-liability paradigm developed by state authorities and could be applied to AI-based content regulation. It highlights that there should be rational, precise, and transparent guidelines in control of the expression on the Internet, which can be applied to algorithmic removals and AI-controlled systems.

Union of India v Anuradha Bhasin (2020).

The Supreme Court in the case of Anuradha Bhasin v Union of India, determined that internet

access is a part of the exercise of Article 19(1),(a). The Court made a condition that the internet shutdowns be determined by need, proportion, and the least restrictions. The importance of this decision lies in the fact that it:

Dismisses access to digital as a facilitating right supporting the freedom of speech, education, and economic engagement.

Places procedural limitations on the state digital disconnection measures, in particular the emergencies and AI governance.

4.2.2 International Case Law and Developments.

In Google Spain v AEPD (Mario Costeja Gonzales), the Court of Justices of the European Union also acknowledged that persons under specific conditions, can demand the de-linking of personal information on search-engine results, on the condition that privacy concerns surpass the test of public-interest-in-information. The case shows:

- Balancing privacy and expression in the algorithmic information environment.
- The treatment of intermediaries (search engines) as quasi-regulators of the speech and memory over the internet.

State v Loomis (Wisconsin, USA)

The Wisconsin Supreme Court in State v Loomis held the use of COMPAS-style and similar risk-assessment algorithms admissible during sentencing, provided the judges are advised of their shortcomings and possible biases. The case:

- Raises the issue of efficiency and equality in AI-based criminal-justice tools.
- Points out why transparency, human control, and procedural protection are necessary when the system of punitive outcomes is impacted by AI.

Cambridge Analytical-related Proceedings.

It is due to the Cambridge Analytica data scandal that triggered regulatory actions and investigations into the matter by EU, UK, and other jurisdictions, following the bulk harvesting

of Facebook user data to support political profiling. These proceedings exposed:

- The threats that psychographic profiling poses and micro-targeted campaigning has on electoral integrity and privacy.
- The necessity to have effective cross-border data-protection and artificial intelligence governance systems that extend beyond national constitutionalism.

4.3 Critical Analysis

4.3.1 Critical Analysis: Doctrinal Coherence vs. Analog-Driven Reasoning

One of the major challenges in the modern legislation of the digital public domain is the still employment of courts and legal systems to apply analog doctrinal arguments in the digital and algorithmic wrongs that are essentially digital. Although constitutional and international principles of human rights have been normatively sound, their application to technologically complex environments tends to become highly constraining in terms of conceptual and operational level.

The fundamental issue with this problem is the disparity of the character of the legal coax and the character of digital technologies. The classic human-rights jurisprudence is premised on the act of the state, the operation of territorial jurisdiction and the decision-making and their human factor. Contrary to the previous point, the digital public sphere is described by automated systems, transnational flows of data and governance of platforms privately. The consequence of this deviation is that the existing doctrines of equality, privacy and free speech have been applied to digital operations by courts without sufficiently modifying to reflect the magnitude, opaqueness, and autonomy of AI systems.

An example of such a bias used in the analysis of the algorithmic bias is the equality jurisprudence under Article 14, which revolves around arbitrariness and reasonable classification. Nevertheless, these forms of doctrines are poorly equipped to question datadriven discrimination, in which bias can be the result not of the intent itself but of the training data or proxy variables or machine-learned associations. The lack of devices to assess the fairness of both data sets and auditors as well as ways to systematically detect bias points to the inefficiency of conventional methods of equality analysis to cope with AI-mediated injuries.

On the same note, courts have long been concerned with the issues of censorship and unconditional curbs on expression by the state, as far as the aspect of freedom of expression is concerned. The digital ecosystem, however, is moving toward the intervention of algorithms and content moderation systems controlled by private actors in speech. The use of doctrines that have been evolved in specific cases Shreya Singhal v Union of India, where vagueness and chilling impacts are highlighted is not entirely accurate in how automated takedowns, shadows banning and prioritisation algorithms are applied. These processes influence the discourse of the masses in a subtle, continuous and often inescapable manner thus avoiding the traditional judicial scrutiny.

A broader flexible framework is offered in the right to privacy as was stated in Justices K.S. Puttaswamy v Union of India which focuses on informational self-determination and proportionality. Nevertheless, AI-based profiling, predictive analysis, and behavioural surveillance still pose some limitations even to this doctrine. The proportionality test, which involves the legality, need and balance, assumes some degree of transparency and accountability that is not always available in the black-box algorithmic systems. In the absence of enforceable explanatory and disclosure needs, it makes no sense that individuals can be meaningfully involved in challenging the breach of their privacy.

The other major disadvantage of analog reasoning is that it is person focused when digital damages are usually systemic and widespread. Algorithms, misinformation, and manipulation of the platform impact millions of people at once, but legal justice still governs the problem of individual complaints and case adjudication. This is a loophole to enforcement, because structural harms of digital systems tend not to be governed amidst the current legal procedure.

Besides, the classical dichotomy between state and non-state actors is becoming more blurred in the online world of the public. Technological corporations execute activities that are highly analogous to the operation of governance, i.e. regulating speech, curation information and opinion formation, although constitutional theories are mainly set up to check government authority. This leads to a high level of accountability gap that is created by the lack of a proper structure of implementing the horizontal human-rights compliance on the private platforms.

Moreover, the time-based and changing character of digital technologies is also challenging to establish with the help of analog legal reasoning. The behaviour of AI systems remains unpredictable since these systems constantly improve themselves through machine learning,

and cannot be controlled with the use of rigid legal norms. Available doctrines based on fixed rules and ex-post adjudication do not inherently work well in the governance of adaptive realtime systems that will result in harm at scale without the legal system taking a hand in the in the meantime.

Such dependence on the analog structures eventually results in the fragmentation and inconsistency of the doctrines. The courts seek to extrapolate their old principles to new facts which leads to piece meal jurisprudence which is not coherent. A case like Puttaswamy, Shreya Singhal, and Anuradha Bhasin all show a sense of judiciary particularly with regard to the digital rights, but all of them do not add up to a unified, AI-aware legal doctrine.

To sum up, the continuation of the analog-driven thinking in the event of the digital change demonstrates one of the weaknesses in the existing human-rights-law. Existing doctrines have the advantage of providing the role they need, but not enough to respond to the peculiarities of AI and platform governance. To achieve doctrinal consistency and inspire the effective protection of rights in the digital era, a change towards more technology-sensitive legal ideas that integrate the concepts of algorithmic and transparency and systemic risks regulation is needed.

4.3.2 Disruption between India and international Standards.

On the global level, policies like the GDPR and the drafted EU AI act implement risk based, horizontal policies towards AI and data security, and a direct requirement regarding the transparency, human control, and remedy. By comparison, the DPDP Act of India is datafocused and lacks:

- Multiple risk-classification system of AI systems (e.g. high-risk vs low-risk uses).
- Nonbinding codes of alcoholic impact-assessment, right-to-bias audits, or administrative and judicial right-to-explanation statutes.

This causes a doctrinal divergence: India agrees with the international norms in principle but falls behind in terms of implementing them into the specifics of rules, which are sensitive to AI.

4.3.3 Loopholes in AI-Governance and Digital Rights.

The project determines some gaps in the doctrines:

Conceptual gaps:

- Lack of statement on rights like algorithmic transparency, explanation and protection, under Articles 14, 19 and 21.
- No explicitly defined status of AI systems in the role of a quasi-state actor in case of doing governance-like activities (e.g.: credit-scoring, welfare distribution).

Weaknesses in regulatory and enforcement:

Disjointed data-protection supervisory efforts between information-security workers, industry oversight bodies and law-courts, causing casing-jurisdiction gaps and accountability-gaps. Few remedies and redress measures to AI-related harms (e.g. deepfakes, automatic denial of welfare by an algorithm, automated hire rejections).

Theoretical–doctrinal tension:

Digital public space is constructed through the influence of the personal platforms and international media, although human-rights based set of obligations continues to be statecentric, which leaves human beings in a discrepancy between the sources of power and the groups to be subject to the directive. The traditional constitutionalism faces a hard time explaining algorithmic amplification, filter bubbles, and disinformation ecosystems, which need new doctrinal instruments when it comes to governance of both the state and the non-state actors.

5. FINDINGS

1. TRANSFORMATION OF PUBLIC SPHERE AND NORMATIVE SHIFT IN HUMAN RIGHTS

➢ The research establishes that how the digital public sphere has been changed and has fundamentally altered the philosophy of human rights shifting them from state-centric and traditionally driven method to platform mediated entitlements.

➢ The traditional human rights paradigm was predicated on clear and identifiable state

actors and clear and discernible violations. However, the new world of digital human rights is characterized by complex and diffuse actors (private entities and AI) and complex and diffuse violations. This is a world characterized by a kind of normative dislocation, where rights to privacy, expression, and equality exist in an algorithmic world and not a physical world.

➢ Inevitably, the concept of human right must be revamped and known as digitally mediated rights, to exist in the real world and not just remain as a mere existence.

2. EXPANSION AND DISTORTION OF CORE HUMAN RIGHTS

- Right to privacy, in its literal sense, has changed to what can now be called as informational self-determination. The research aimed to establish that how privacy as a concept has evolved from protection against state intrusion to protection against mass data extraction from backup clouds etc., surveillance capitalism and AI profiling.

- Cases such as ***KS Puttuswamy***, established that informational privacy may not always be a blanket, and AI driven profiling surpasses the traditional way of proportionality frameworks, majorly because of the lack of clarity.

- The ***Cambridge Analytica scandal*** emphasized on how data misuse can influence political ideologies, democratic processes, revealing that how privacy violations now have a collective consequence, rather than merely an individual impact.

- The freedom of expression, has evolved as a concept to an algorithmically mediated speech. It does not remain merely as a state centric censorship, but has developed to an algorithmic amplification, suppression, and visibility control.

- The research demonstrates the significance of the fact that platform algorithms function as regulators of free speech. ***Shreya Singhal*** discusses the issue of vagueness in law; however, it does not discuss the lack of transparency in algorithmic moderation since 2015 was a decade ago and the digital sphere was still evolving back then.

- Equality and non-discrimination within the AI systems reproduces structural inequalities through predictive analysis and bias within its algorithmic data sets. This majorly affects the hiring, policing and welfare distribution systems.

- The research also points out at the fact that traditional doctrines of equality which were based on intent and classification are now inadequate to strain through the systemic and statistical discrimination.

- The case of ***Dutch Syri*** emphasized and illustrated that how such systematic algorithmic governance may lead to violation of privacy and equality due to the inconsistency in transparency and proportionality.

- The access to information was a right which has reformed as a facilitating right in sphere of digital access as concluded in the case of ***Anuradha Bhasin*** by recognizing the ethical usage of internet access. It also indicated that if digital equity is not ensured, then the formal recognition of such access is insufficient, hence creating a persisting digital divide.

3. RESHAPING RIGHTS: ROLE OF MEDIA AND GLOBALIZATION

- Media convergence and globalization augmented both empowerment and vulnerability simultaneously.

- On one end, the globally used digital platforms enabled transnational mobilization and importance of consented participation; the other gave rise to facilitating misinformation, unsolicited surveillance, and manipulation on a large scale.

- Human rights are hence, no longer limited to domestic boundaries, and rather operate within global data sets which are controlled by various multinational corporations.

- Such inconsistencies lead to jurisdictional crisis, where violations occur at cross borders, but their legal remedies are territorially limited.

4. DOCTRINAL INADEQUACIES (INDIA AND INTERNATIONAL)

- The existing constitutional and international doctrines may be conventionally relevant, but not operative sufficiently. Analog reasoning to digital harms create fragmented jurisprudence causing indefinite loopholes for addressing legitimate inconsistencies.

- Such disparity arises because traditional law assumes human-decision makers, while

AI deals with autonomous systems. Legal frameworks address individual harms, where digital harms are essentially collective and systemic.

- India depends on its constitutional provisions (Article 14, 19, 21), following which came into existence the DPDP act (2023) on data protection and consent. However, it lacks on addressing the issues of algorithmic transparency, risk classification within the AI systems, and the right to explanation.

- The international standards such as the EU model, adopt a right based and a risk oriented framework by recognizing emerging rights such as right to explanation of the automated decisions, transparency and accountability obligations, embedding fundamental rights as a regulatory threshold across the usage of AI.

- Despite doctrinal alignment, a divergence is created in which India lags in operationalizing digital rights.

5. DEVELOPMENT OF ALGORITHMIC GOVERNANCE AND ACCOUNTABILITY GAPS

- The AI systems now increasingly perform governance like functions, such as decision making make in welfare and sovereign functions, criminal justice system, and scientific information. However, these systems operate without any explanation, judicial oversight, and transparency.

- In the case of ***State vs Loomis,*** the risk of opaque algorithmic decision making raised concerns regarding the idea of due process. Algorithmic opacity undermines judicial review and fair exercise of digital human rights.

- Conceptual gaps such as the absence of explicit recognition of the right to algorithmic transparency, right to explanation, and right against automated discrimination raise serious concerns regarding the lack of clarity on status of the private platforms acting as quasi state actors.

- Weak institutional mechanisms create enforcement gaps and cross border data violations which results in a fragmented regulatory oversight leading to a vacuum in accountability and compliance.

- Human rights, although remain state centric, digital powers are platform centric which creates a gap between power and responsibility, hence leading to undermining enforcement mechanism.

6. RECONCEPTUALIZED DIGITAL HUMAN RIGHTS FRAMEWORK AND RESISTRIBUTION OF POWER (SUGGESTIONS)

- The research aimed to target revamping of human rights in the digital public sphere which must be grounded in both doctrinal evolution and recognizing shifting and evolving power structures. It necessitates a framework that is able to integrate both the substantive expansion of human rights as well as the structural governance reforms.

- Substantive rights must evolve:

- *Privacy* should include data protection and sovereignty against mass surveillance.

- *Equality* must be safeguarded against any possible algorithmic bias and automated discrimination.

- *Accountability* must be expressed for platform based mediated visibility.

- Procedural safeguards are essential to ensure enforceability mechanism by creating algorithmic transparency, enabling individuals to cross question automated decision, and human vigilance to counter unchecked automation and protect accountability. Absence of such safeguards lead to a due process deficit leading to complexity.

- Structural reforms such as establishing AI regulating authorities, cross border governance mechanisms, and technology sensitive framework would ensure that evolving digital public sphere does not compromise constitutional values, accountability and human dignity.

CONCLUSION

As said by Nick Bostrom *"The real risk with AI and digital world isn't malice, but competence"*. This evolving future which we are already living in does not mark a mere technological shift, but a turning point in the idea of human rights. The migration of discourse,

governance, and digitally mediated decision making fundamentally disrupts the tradition paradigm of human rights, which are no longer practiced in neutral environments, but opaque and data driven architectures which shapes behaviour, access and autonomy scale. The evolvement of legal doctrines must be in tandem with technological realities where both the state and non-state actors must be held accountable. Unless, law is able to reclaim its regulating authority, digital systems may wipe out the freedoms which they have a duty and responsibility to enhance.

Therefore, it is imperative to reconceptualize human rights in order to ensure human dignity, autonomy, while making democratic values central in the digitally increasing algorithmic world.

BIBLIOGRAPHY

1. National Human Rights Commission, Human Rights Protection Framework in India, nhrc.nic.in/human-rights-framework

2. Office of the United Nations High Commissioner for Human Rights, Freedom of Expression and Opinion, https://www.ohchr.org/en/topic/freedom-expression-andopinion

3. European Network of National Human Rights Institutions, Key Human Rights Challenges of Artificial Intelligence, https://ennhri.org/ai-resource/key-human-rightschallenges/

4. United Nations Regional Information Centre for Western Europe, Protecting Human Rights in an AI-Driven World, https://unric.org/en/protecting-human-rights-in-an-aidriven-world/