Page: 2710-2732 *URL: www.lijdlr.com*

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 1

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.120

RETHINKING CONSTITUTIONAL REMEDIES UNDER ARTICLE 32 AND ARTICLE 226 FOR GENERATIVE AI- CAUSED FUNDAMENTAL RIGHTS VIOLATIONS

Kaveri[1]

I. ABSTRACT

It can read faster, think faster, comprehend faster- "Gen- AI" clearly has reduced human effort, a little too much. Gen- AI's rise in recent times is era defining and as it goes, everything comes with its own unique challenges. To address this, Gen-AI needs to be legislated first, properly regulated. But there needs to be (initially) a practical redressal system for Fundamental Rights Violations caused by Generative AI technology. For this, we do have Article 32 and Article 226, but not without its own grey areas. As GenAI systems, operated by corporate entities, increasingly cause reputational, discriminatory, and financial harms, the existing legal frameworks particularly the definition of 'State' under Article 12 and traditional writ remedies do not give a complete answer to the problem at hand. The judgement in Kaushal Kishor v. State of U.P. (2023) has established that Article 19 and Article 21 can be enforced against Private entities, but how does one build a "chain of causation" in Gen-AI fundamental rights' violations, for aggrieved party to bring several parties into defendant/respondent side. This article posits that the Indian Constitution possesses the inherent dynamism to bridge this gap and our Judiciary can answer these challenges and bring clarity to it, via Judicial Interpretation and some Judicial Creativity. We should evaluate if private entities exercising 'functional sovereignty' via GenAI can be brought under an expanded Article 12 ambit. And could the courts recognise a new constitutional tort of AI-based reckless or simple negligence?

II. KEYWORDS

Generative Artificial Intelligence, Gen-AI violations, Constitutional remedies, Fundamental Rights, Constitutional Torts.

[1] LL.M (Constitutional law and Administrative Law), 2nd Semester, Student at Gujarat National Law University, Silvassa (India). Email:kaveri25smcal09@gnlus.ac.in

 (ISSN: 2583-7753)

III. INTRODUCTION

For much of our history, it was a deeply entrenched presumption that the province of artistic and creative endeavour like the composition of poetry, the authoring of software, the design of fashion, or the creation of music, was an exclusively human domain. This long-held assumption has been profoundly unsettled by recent advancements in artificial intelligence. Today, AI demonstrates a capacity to generate novel content of such sophistication that it is often indistinguishable from that of human craftsmanship.

A prudent point of departure is to establish a clear understanding of "Generative Artificial Intelligence" or "Gen-AI", delineating both its capabilities and its limitations. The term 'Generative AI' denotes a suite of computational techniques capable of producing ostensibly new and meaningful content, be it text, imagery, or audio—derived from extensive training datasets.[2] The recent fervour has largely centred on Large Language Models (LLMs), such as those underpinning ChatGPT and Bing AI, alongside image-generation systems like DALL-E and Stable Diffusion.[3] These tools empower users to produce text of a professional calibre and compelling imagery through simple English-language instructions. The purview of these systems extends beyond the artistic, where they emulate writers and illustrators; they are also poised to serve as intelligent assistants in question-answering capacities.[4] Potential applications range from IT help desks, where they may support transitional knowledge work, to more quotidian tasks such as providing culinary or medical guidance.[5]

In 2023, a study by Goldman Sachs Research suggests that Generative AI could elevate global GDP by 7%, while simultaneously exposing the equivalent of approximately 300 million full-time jobs to automation, with the extent of actual displacement

[2] A. Bordas et al, 'WHAT IS GENERATIVE IN GENERATIVE ARTIFICIAL INTELLIGENCE? A DESIGN-BASED PERSPECTIVE' (2024) 35 Research in Engineering Design 427
[3] J. Euchner, 'GENERATIVE AI' (2023) 66(3) Research-Technology Management 71
[4] F.J. García Peñalvo and A. Vázquez Ingelmo, 'WHAT DO WE MEAN BY GENAI? A SYSTEMATIC MAPPING OF THE EVOLUTION, TRENDS, AND TECHNIQUES INVOLVED IN GENERATIVE AI' (2023) 8(4) IJIMAI 7
[5] S. Feuerriegel et al, 'GENERATIVE AI' (2024) 66 Business & Information Systems Engineering 111

contingent upon the pace and nature of technological adoption.[6] Undoubtedly, this portends profound implications. On one hand, the projected 7% GDP growth heralds a new era of productivity, innovation, and potential economic abundance driven by the automation of complex cognitive tasks. On the other, the large-scale exposure of jobs to automation suggests a formidable challenge to the very structure of the knowledge economy, the precise impact of which will depend on how such technologies are integrated into existing labour markets, necessitating a fundamental re-evaluation of the nature of work, the distribution of wealth, and the societal safeguards required to manage a transition of such scale responsibly. It is therefore incumbent upon us to navigate the attendant risks and to steer the development and application of this powerful technology towards responsible and sustainable ends.

However, this socio-economic transition is marked by a far more fundamental constitutional dilemma. This research article is compelled by a pressing constitutional imperative: the inadequacy of existing legal provisions and precedents to hold power accountable in the age of Generative Artificial Intelligence. The central problem it confronts is the emerging accountability gap between the immense power wielded by private entities through Generative AI and the current scope of the constitutional remedies.

To address this, Gen-AI needs to be legislated first, properly regulated. But there needs to be (initially) a practical redressal system for Fundamental Rights Violations caused by Generative AI technology. For this, we do have Article 32 and Article 226, but not without its own grey areas. This is not because the rights themselves are diminished, but because the nature of the violator and the character of the violation have transformed beyond the original contemplation of the Indian Constitution. When harm is caused not by a direct state actor but by the opaque, unpredictable output of a corporate-owned AI models, the pathways to justice become fraught with uncertainty.

[6] Goldman Sachs, 'GENERATIVE AI COULD RAISE GLOBAL GDP BY 7%' (Goldman Sachs, 5 April 2023) https://www.goldmansachs.com/insights/articles/generative-ai-could-raise-global-gdp-by-7-percent

As GenAI systems, operated by corporate entities, increasingly cause reputational, discriminatory, and financial harms, the existing legal frameworks particularly the definition of 'State' under Article 12 and traditional writ remedies do not give a complete answer to the problem at hand. The judgement in *Kaushal Kishor Case (2023)*[7] has established that Article 19 and Article 21 can be enforced against Private entities. But today, we have more questions on the ratio, than the uniformity in interpretation of law, that this judgement should have provided.

How does one build a "chain of causation" in Gen-AI fundamental rights' violations, for aggrieved party to bring several parties into defendant/respondent side? Whether or not, private entities exercising 'functional sovereignty' via GenAI can be brought under an expanded Article 12 ambit? Can Indian Constitution's inherent dynamism bridge this gap? What scope of Judicial Creativity is required for such a task? And could the courts recognise a new constitutional tort of AI-based reckless or simple negligence?

A. Research Problem

This research is compelled by a fundamental and urgent constitutional dilemma: the inadequacy of existing legal frameworks to hold power accountable in the age of artificial intelligence. The central problem it confronts is the emerging accountability chasm between the immense power wielded by private entities through generative AI. The citizen's right to approach the Supreme Court or High Court under Article 32 or Article 226 for the enforcement of fundamental rights faces potential ambiguity. This is not because the rights themselves are diminished, but because the nature of the violator and the character of the violation have transformed beyond the original contemplation. Harm is caused not by a direct state actor but by the opaque, unpredictable output of a corporate-owned GenAI. This gives rise to several intertwined dimensions of the core research problem of this study:

1. When private corporations control AI systems that govern access to essential public services, opportunities, and information, they exercise a

[7] Kaushal Kishor v. State of U.P., (2023) 4 SCC 1

form of de facto sovereignty by having enormous impact on public interest. The current interpretation of 'State' under Article 12 risks creating a zone of unaccountable private power, leaving citizens without recourse against violations that are fundamental in everything but their source.

2. The inherent opacity of generative AI models makes it exceptionally difficult, if not impossible, for an individual victim to establish the precise chain of causation required by traditional constitutional tort law as is understood currently. This creates an insurmountable evidentiary barrier, rendering the right to a remedy theoretically intact but practically unenforceable.
3. The traditional writs, while versatile, were designed for a different era of governance and malfeasance. They may be ill-suited to provide effective relief for novel, and systemic harms like mass misinformation, algorithmic discrimination, or the unauthorized appropriation of personal data for model training. The judiciary must evolve suitable framework to protect interests of citizens.
4. The expanse of Article 21 is weakened if a citizen cannot understand the reason for an automated decision affecting their livelihood or reputation, nor challenge it through a fair redressal mechanism. The problem is the absence of a constitutional obligation on private actors to build transparency and appeal into systems that functionally adjudicate rights.

B. Research Objectives

To ensure that the fundamental right to a constitutional remedy, which is the cornerstone of Indian democracy enshrined in Articles 32 and the constitutional right to seek such redressal under the wider jurisdiction of Article 226, retains its supreme efficacy in the face of a novel challenge of Generative Artificial Intelligence, this research has following objectives:

1. To determine the jurisprudential viability of expanding the definition of 'State' under Article 12 of the Constitution of India, to encompass private entities whose generative AI systems effectuate fundamental rights

violations, particularly where such systems operate in a manner functionally analogous to or deeply intertwined with governmental functions or public data.

2. To construct a legal framework for the attribution of liability for harms including reputational damage, discriminatory practices, and psychological or financial distress caused by the opaque outputs of generative AI, thereby establishing a clear causal pathway to enable affected individuals to seek redress under Articles 32 or 226.
3. To conceptualise and propose novel, adapted forms of constitutional remedies beyond the traditional writs, which are specifically tailored to provide effective and just relief for the unique nature of harms caused by generative AI, such as systemic misinformation, privacy violations, and intellectual property infringement.
4. To delineate the precise infringements upon the right to privacy under Article 21 arising from the use of personal data in AI training sets and the generation of synthetic content, and to articulate the corresponding constitutional remedies available to citizens to seek redress.
5. To interpret the rights under Article 21 as imposing a positive constitutional obligation upon private corporations to embed principles of algorithmic transparency, explainability, and a meaningful right to appeal within their generative AI systems, thereby safeguarding an individual's life and livelihood from arbitrary automated decision-making.
6. To delineate the contours of Public Interest Litigation (PIL) in this context, by defining the proper "locus standi" for systemic challenges and articulating the structure of a petition that compels legislative or executive action to address widespread harm caused by discriminatory AI models.

C. Research Questions

This research, at its very core, seeks to navigate the complex and evolving intersection of constitutional law and artificial intelligence. The questions that follow are the intellectual signposts that guide this scholarly journey, born from a recognition that the Right to constitutional remedy under Article 32 (SC jurisdiction) and Article 226

(HC jurisdiction) must be re-examined in the face of Gen AI. The following are research questions:

1. To what extent can the SC and HCs expand the definition of 'state' under Article 12 and therein, the enforceability of fundamental rights, to hold a private entity accountable for fundamental rights violations caused by its Gen AI, particularly when the AI's operation is inextricably linked to government functions or public data?
2. How to establish direct liability for harms such as reputational damage, discriminatory practises like ageism at workplace, caused by the unpredictable and opaque outputs of a generative AI be traced to the liable party (State or/and Private Corporations), thereby enabling an affected individual to seek a constitutional remedy under Article 32 or 226?
3. Given the unique nature of Gen AI-caused harm (e.g., rampant misinformation, privacy violations, IPR violations), What new forms of Constitutional Remedies, if beyond the traditional writs, could the SC and HC develop to provide effective relief and thereby, safeguard fundamental rights?
4. In what specific ways does the use of generative AI infringe upon the right to privacy under Article 21, and what constitutional remedies are available to prevent the unauthorized use of personal data for training purposes or to challenge the generation of personally identifiable synthetic content?
5. How can the expansive rights under scope of Article 21 and the principles of natural justice be interpreted to impose a constitutional obligation on private companies using generative AI to ensure algorithmic transparency, explainability, and the right to appeal an automated decision that affects a person's life or livelihood?
6. What will a petition in the nature of PIL look like demanding legislations against or/and violations caused by Gen AI? In cases of systemic or widespread harm caused by a discriminatory generative AI model, what is the proper locus standi for filing a Public Interest Litigation (PIL) under Article 32?

D. Research Hypothesis

To navigate this uncharted legal terrain, the author advances the following hypotheses. These propositions aim to recalibrate understanding of right to constitutional remedy and principles of administration of justice, for the age of artificial intelligence.

1. That the exercise of 'functional sovereignty' by a private entity through the control of a gen AI system that governs access to essential public opportunities, resources, or information creates a sufficient nexus to bring such an entity within the expanded ambit of 'State' under Article 12, thereby making its actions subject to fundamental rights challenges under Articles 32 and 226.
2. That the SC and HCs, in exercise of their powers under Article 32 and Article 226 respectively, can and should recognize a new 'constitutional tort' of algorithmic negligence, imposing strict liability on developers and deployers of generative AI for fundamental rights violations arising from a failure to meet a judicially-defined standard of care in design, testing, and deployment.
3. That a private corporation's failure to provide the procedural safeguards of algorithmic transparency, explainability, and a right to appeal as mandated by a purposive interpretation of Article 21, will create a rebuttable presumption of liability for any subsequent fundamental rights violation caused by its generative AI system, effectively shifting the evidentiary burden onto the corporation in a subsequent writ petition.

E. Research Methodology

This research will employ a qualitative doctrinal legal research methodology. The primary aim is to engage in a critical and systematic analysis of legal sources to identify, interpret, and synthesise legal principles, with the ultimate goal of constructing a coherent and persuasive jurisprudential argument.

The core of the investigation will involve the critical examination of primary sources of law. This includes a meticulous analysis of relevant constitutional provisions

namely Articles 12, 14, 19, 21, 32, and 226 of the Indian Constitution, and the seminal judicial precedents that have shaped their interpretation. Landmark Supreme Court and High Court judgments will be dissected to trace the evolution of doctrines such as the definition of State, the expansion of Article 21, and the judiciary's innovative use of writ jurisdiction.

This will be supplemented by a review of pertinent statutory frameworks and any emerging regulatory guidelines concerning artificial intelligence.

To contextualise and strengthen the analysis, the methodology will also incorporate a review of secondary sources. This encompasses engaging with scholarly literature from leading legal academics, theoretical frameworks from international human rights law concerning corporate accountability, and policy papers. The synthesis of these primary and secondary materials will facilitate a robust doctrinal analysis, enabling this research to not only describe the current legal landscape but also to persuasively argue for the novel legal innovations and interpretations proposed in its hypotheses.

F. Literature Review

In formulating this research, the author has engaged with an extensive body of scholarly literature. The established frameworks and critical insights of the following authors provide an invaluable foundation upon which to construct a novel pathway for addressing the central research questions outlined in this research proposal.

1. **Article titled "Corporate Accountability and Liability for International Human Rights Abuses: Recent Changes and Recurring Challenges" written by Emeka Duruigbo in 2008:** This research is situated within the critical scholarly discourse on holding private power accountable for systemic harms, a challenge extensively detailed in international human rights law.[8] This study transposes this discourse into the novel realm of algorithmic governance, arguing that the accountability gap Duruigbo

[8] Emeka Duruigbo, 'Corporate Accountability and Liability for International Human Rights Abuses: Recent Changes and Recurring Challenges' (2008) 6(2) Northwestern Journal of International Human Rights

identifies is exponentially magnified by the opaque nature of generative AI. While engaging with Indian constitutional scholarship on expanding the definition of 'State' under Article 12, this research seeks to fill a distinct gap by exploring how the existing machinery of constitutional remedies, specifically the writ jurisdictions under Articles 32 and 226 can be dynamically interpreted to provide immediate redress, even in the absence of new legislation.

2. **Article titled "'Two Visions for Data Governance: Territorial vs. Functional Sovereignty' by F. Pasquale in Oxford University Press 2023:** Frank Pasquale's "Two Visions for Data Governance: Territorial vs. Functional Sovereignty" (2023) provides a critical theoretical anchor for this research, particularly its first hypothesis.[9] Pasquale's articulation of 'functional sovereignty' offers a robust conceptual framework to argue for expanding Article 12's definition of 'State'. His work justifies treating private entities exercising sovereign-like control over public digital spaces as state actors, directly informing this study's aim to bridge the accountability gap in generative AI governance through constitutional means.
3. **Article written in Live Law titled 'A Case for Harmonizing Gen AI and The Copyright Regime' on by Nikhil Narendran:** Nikhil Narendran's Live law article, while primarily engaging with copyright law, presents a crucial counterpoint that profoundly enriches the constitutional dimensions of this research.[10] By arguing that copyright is a limited statutory right designed to balance creator incentives with public access and innovation, Narendran implicitly challenges the absolutist framing of generative AI's data usage as a purely exploitative harm. This perspective is vital for this study's fourth objective, which examines fundamental rights violations under Article 21. It necessitates a more nuanced constitutional analysis: rather than assuming

[9] F. Pasquale, 'Two Visions for Data Governance: Territorial vs. Functional Sovereignty' in F. Pasquale (ed), Data Sovereignty (Oxford University Press 2023) 35.
[10] Nikhil Narendran, 'A Case For Harmonizing Gen AI And The Copyright Regime' (Live Law, 24 Mar 2025) https://www.livelaw.in/articles/case-harmonizing-gen-ai-copyright-regime-287263

all unauthorized data use for training is a per se violation, the research must now interrogate whether such use constitutes a proportionate limitation on the right to property or privacy in service of the public interest such as technological progress, access to knowledge, and the prevention of AI bias and whether existing constitutional remedies like fair dealing can be adapted to create a balanced, rights-based framework for AI governance that respects both individual rights and collective technological advancement.

4. **Article written by Pranjal Chaturvedi and Dr. Suhasini in Live Law on 27 Feb 2025 titled, "AI And Personhood: Navigating Legal Rights and Responsibilities in the Age of Intelligent Machine":** provides a critical philosophical and legal inquiry that serves as a necessary boundary for the present research. By engaging with the complex debate on whether advanced AI systems should be granted any form of legal personhood a concept that would fundamentally alter liability frameworks the authors highlight a profound jurisprudential frontier. However, their exploration of attributing responsibility to AI directly reinforces the central constitutional premise of this study: that in the current landscape, accountability must reside firmly with the human and corporate entities that develop, deploy, and benefit from these systems. This research therefore builds upon their foundational work by accepting their conclusion that AI itself is not a rights-bearing entity, and instead focuses its inquiry on the urgent, practical question they leave open: how to constitutionally attribute liability and enforce fundamental rights against the corporations whose "intelligent machines" cause demonstrable harm, ensuring that the veil of technological complexity does not become a shield against constitutional accountability.

IV. PRACTICAL SCENARIOS OF GEN-AI CAUSED FUNDAMENTAL RIGHTS VIOLATIONS

The rise of Generative Artificial Intelligence (Gen-AI), exemplified by sophisticated Large Language Models (LLMs) like ChatGPT, marks a significant technological leap

beyond earlier, rule-based systems. Unlike its predecessors, Gen-AI's ability to "think" intelligently, produce human-like content, and operate on a vast scale introduces unprecedented challenges to fundamental rights. The very mechanisms that make Gen-AI powerful its reliance on massive, scraped datasets and its capacity for realistic, rapid content generation are the conduits for rights violations across multiple domains, primarily privacy, expression and occupational threat.

The right to privacy is fundamentally challenged by Gen-AI, particularly through the creation of highly realistic synthetic media, known as deepfakes, and the potential for the misuse of personal data ingested during the training process. Deepfake technology leverages Gen-AI (specifically Generative Adversarial Networks or GANs and variational autoencoders) to synthesize images, video, and audio that are virtually indistinguishable from authentic media. This poses a direct threat to an individual's right to identity and reputation.

One of the most egregious violations is the creation of "Non-Consensual Deepfake Imagery" particularly the "Non-Consensual Deepfake Pornography", predominantly targeting women. This constitutes a severe violation of bodily integrity, dignity, and privacy, inflicting profound psychological harm and online harassment.[11] The ease with which an image of a private individual can be manipulated to appear in a compromising video is a clear infringement on personal autonomy.[12]

Gen-AI voice cloning, often requiring only a few seconds of a person's voice, has been used in fraudulent schemes. This is legally understood under the term "Malicious Impersonation". For instance, sophisticated deepfake audio has been employed to impersonate CEOs to authorize fraudulent financial transfers or to mimic relatives to perpetrate scams against family members.[13] As highlighted by the *Arijit Singh case*[14]

[11] Rebecca Umbach, et. al., 2024. NON-CONSENSUAL SYNTHETIC INTIMATE IMAGERY: PREVALENCE, ATTITUDES, AND KNOWLEDGE IN 10 COUNTRIES. IN PROCEEDINGS OF THE CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (CHI '24), May 11--16, 2024, Honolulu, HI, USA

[12] Ibid

[13] Bhattacharya, Saurav & Dodda, Suresh & Khanna, Anirudh & Panyam, Sriram & Balakrishnan, Anandaganesh & Jindal, Mayank. (2024). GENERATIVE AI SECURITY: PROTECTING USERS FROM IMPERSONATION AND PRIVACY BREACHES. INTERNATIONAL JOURNAL OF COMPUTER TRENDS AND TECHNOLOGY. 72. 51-57. 10.14445/22312803/IJCTT-V72I4P106

[14] Arijit Singh v. Codible Ventures LLP, 2024 SCC OnLine Bom 2445

(2024) in India, the unauthorized replication of a person's voice and likeness for commercial gain or malicious intent infringes upon their personality rights and right of publicity, which are often legally recognized extensions of privacy and expression rights.

Deepfakes pose a profound threat to democratic processes and freedom of expression by undermining trust in public information. Fabricated videos of politicians making inflammatory statements or engaging in unethical behaviour can be released just before an election, effectively defaming individuals and manipulating public opinion without the possibility of an immediate, credible retraction. This directly harms their reputation and the public's right to truthful information, a prerequisite for informed political expression.

The training of massive LLMs involves data scraping, the automated extraction of content from the public internet.[15] While the data is often anonymized or aggregated, the sheer scale of the operation and the nature of the scraped content still raise privacy concerns.[16] Training datasets can inadvertently capture sensitive personal data or confidential communications that were once accessible on a public webpage (e.g., in a forum post, an unsecure blog comment, or a leaked document).[17] When the model is prompted, it can sometimes regurgitate or reproduce portions of this sensitive data, exposing individuals and organizations to harm.[18]

Privacy regulations, such as the General Data Protection Regulation (GDPR), as well as India's Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025, include the Right to Erasure (Right to be Forgotten), consent-based processing obligations, and principles of data minimisation.[19] Gen-AI models, once trained, are notoriously difficult to modify to erase specific data points, as the information is not stored discretely but is encoded diffusely across billions of model

[15] Mustapha, Shehu & Man, Mustafa & Wan Abu Bakar, Wan Aezwani & Yusof, Kamir & ahmad sabri, Ily. (2024). DEMYSTIFIED OVERVIEW OF DATA SCRAPING. INTERNATIONAL JOURNAL OF DATA SCIENCE AND ADVANCED ANALYTICS. 6. 290-296. 10.69511/ijdsaa. v6i6.205
[16] Ibid
[17] Ibid
[18] Ibid
[19] Ryngaert, Cedric & Taylor, Mistale. (2020). THE GDPR AS GLOBAL DATA PROTECTION REGULATION? AJIL Unbound. 114. 5-9. 10.1017/aju.2019.80.

parameters, thereby creating practical compliance challenges with both the GDPR and India's Digital Personal Data Protection Act, 2023, particularly in relation to erasure and correction rights of data principals.[20] This makes compliance with fundamental data protection rights technically challenging, if not practically impossible, once the data has been ingested.

Under the Digital Personal Data Protection Act, 2023, data fiduciaries are obligated to process personal data on the basis of valid consent and ensure purpose limitation, while the DPDP Rules, 2025 further operationalise compliance mechanisms. However, the framework exhibits limitations in the context of generative AI, including exemptions relating to publicly available data and the absence of explicit obligations concerning algorithmic transparency or explainability in AI systems.

While the GDPR offers a robust comparative benchmark, the Indian framework under the Digital Personal Data Protection Act, 2023 must be central to any constitutional analysis, particularly as it derives normative force from the right to privacy recognised under Article 21. Nevertheless, its current design does not fully address the structural opacity and accountability challenges posed by generative AI, thereby reinforcing the need for strengthened constitutional remedies under Articles 32 and 226.

The generative capability of Gen-AI places it directly in conflict with the fundamental rights of human creators, their ability to earn a living through their creative expression. The reliance on scraped data for model training has fuelled numerous high-profile lawsuits. Though this is in realm of Intellectual property, it also talks a lot to the Freedom of Expression and Freedom of trade & Occupation, provided under article 19.

The efficiency and sophistication of Gen-AI pose a direct occupational threat to human creators and knowledge workers, indirectly challenging their right to work and their ability to sustain themselves through their professional expression. The ability of LLMs to summarize articles, write code, or draft routine correspondence means that many tasks previously performed by copywriters, paralegals, junior programmers,

[20] Ibid

and journalists are becoming heavily automated. This mass automation can lead to job displacement or significant downward pressure on wages for creative professionals.

Even where a job is not entirely eliminated, the market value of a human-created work is diluted when a Gen-AI system can produce a similar work instantly and at near-zero marginal cost. This shift threatens the economic viability of entire professions, from freelance graphic designers (whose styles can be replicated by image generators) to authors (whose books were used to train the models now capable of producing imitative prose). The lack of a clear, compulsory licensing and compensation structure for the use of copyrighted works in training data means that the foundational right to profit from one's own expression is being eroded.

The process of data scraping involves making billions of copies of copyrighted works (articles, books, images, code, music) to train the LLMs.[21] This constitutes unauthorized reproduction and the creation of derivative works, infringing their copyright. Commercial use to build a multi-billion-dollar product is not protected by exceptions like "fair use," as the Gen-AI output directly competes with and substitutes for the original copyrighted works.[22]

Though Gen-AI is designed to generate novel content, its output can occasionally resemble or directly duplicate specific copyrighted material from its training set. When a Gen-AI model generates a song that copies a unique vocal style, or an image that closely mimics a specific artist's distinctive composition, the output itself becomes a clear act of infringement.

This is particularly relevant in cases involving voice cloning, where the unique expression of a performer's voice is illegally replicated. Gen-AI models can perpetuate and even amplify existing societal biases, which are embedded in the massive, historically skewed datasets upon which they are trained. This leads to violations of the fundamental right to equality and non-discrimination.

When Gen-AI is used in high-stakes contexts such as screening job applications, determining loan eligibility, or assisting in medical diagnoses biased outputs can lead

[21] Supra (note 11)
[22] Supra (note 11)

to discriminatory outcomes.[23] For example, a recruitment LLM trained on historical hiring data, which disproportionately favoured one demographic, might learn to devalue resumes containing indicators associated with another demographic, resulting in systemic discrimination in the right to work. Gen-AI image generators often produce stereotypical or biased representations when prompted with generic terms (e.g., generating only male images for a prompt like "great leader" or producing images with specific, stereotypical attributes for certain professions or ethnic groups).[24] This reinforcement of harmful stereotypes constitutes an indirect violation of the right to dignity and equality for the misrepresented groups.[25] This is a critical risk, reflected in binding regulatory frameworks such as the European Union's Artificial Intelligence Act (Regulation (EU) 2024/1689), which classifies AI systems used in areas like employment as 'high-risk' due to their potential to interfere with fundamental rights. The Regulation, in force since August 2024 with phased implementation timelines, establishes enforceable compliance obligations for such systems.[26]

In conclusion, the practical scenarios of Gen-AI-caused fundamental rights violations are not merely hypothetical; they are actively occurring in the realms of personal privacy (deepfakes, data leaks), creative occupations (copyright infringement, market dilution), and social justice (algorithmic bias). Addressing these challenges requires a concerted legal and ethical framework that mandates transparency, provides effective redress for harm, and rebalances the rights of technology developers with the fundamental rights of the individuals whose data and work fuel the Gen-AI revolution.

[23] Belenguer, Lorenzo. (2022). AI BIAS: EXPLORING DISCRIMINATORY ALGORITHMIC DECISION-MAKING MODELS AND THE APPLICATION OF POSSIBLE MACHINE-CENTRIC SOLUTIONS ADAPTED FROM THE PHARMACEUTICAL INDUSTRY. AI and Ethics. 2. 771-787. 10.1007/s43681-022-00138-8
[24] Ibid
[25] Ibid
[26] Ibid

V. IMPLICATIONS OF KAUSHAL KISHOR CASE (2023) IN GEN-AI VIOLATIONS

The Constitution Bench ruling in *Kaushal Kishor v. State of U.P.*[27] delivered a landmark affirmation: fundamental rights, particularly those under Article 19 (Freedom of Speech and Expression) and Article 21 (Right to Life and Personal Liberty), are enforceable against non-State actors, including private individuals and entities. This principle, known as the "*Horizontal application of fundamental rights*", profoundly shifts the legal landscape, providing a crucial constitutional hook for addressing the harms caused by private technology companies and Gen-AI systems that operate outside the traditional confines of State power.

Before Kaushal Kishor, victims of rights violations by private entities such as data leaks, deepfakes, or algorithmic bias perpetrated by tech corporations were largely relegated to seeking remedies under ordinary common law (torts, defamation, contracts) or specific statutory law (like the IT Act). These remedies are often slow and lack the fundamental gravity of constitutional redress. Gen-AI exacerbates this problem, as its primary actors the large language model developers and major social media platforms are all *non-state entities*. The Horizontal application established by the majority opinion in *Kaushal Kishor* allows a citizen to directly claim a violation of their constitutional rights, specifically their Right to Privacy and Right to Dignity (both integral to Article 21), against a private Gen-AI developer or a malicious individual user creating harmful synthetic content.

For instance, if a deepfake video is created and distributed by a private actor, violating a victim's dignity and privacy, this 2023 judgement theoretically empowers the victim to approach the High Court or Supreme Court via a writ petition, claiming a direct violation of their Article 21 rights by the private individual. This elevated constitutional remedy is far more potent than a mere tort claims for damages, as it forces accountability at the highest level of jurisprudence. Similarly, claims concerning data scraping where private companies use copyrighted or personal data to train

[27] (2023) 4 SCC 1

LLMs can now be framed as a direct breach of the right to privacy under Article 21 by the private technology company itself.

Despite its transformative potential, the Kaushal Kishor judgment faces significant criticism, with some legal scholars arguing it represents a "bad judgment" due to interpretive ambiguities and procedural hurdles.

The primary challenge lies in the lack of clarity regarding the extent and mechanism of horizontal application. As Justice B.V. Nagarathna noted in her partly dissenting opinion[28], extending the enforcement of Articles 19 and 21 against all private citizens may unduly blur the well-defined boundaries between public law (constitutional claims) and private law (common law claims), potentially leading to an "unbounded" expansion of writ jurisdiction.[29]

This ambiguity is particularly problematic for regulating Gen-AI. When a court attempts to apply the Right to Dignity (Article 21) against an alleged violation caused by a private AI developer's Freedom of Speech (Article 19(1)(a)), it is forced to undertake a complex constitutional balancing act without clear legislative guidelines. The majority judgment did not sufficiently define the criteria for when a constitutional court should intervene against a private actor, especially when alternative and efficacious common law remedies already exist.

Furthermore, the ruling could potentially complicate the regulation of Gen-AI by transforming every dispute over defamatory AI outputs or copyright infringement into a constitutional question, thereby demanding complex judicial interpretation of technological failures rather than relying on the precision of statutory instruments. While *Kaushal Kishor* provides the indispensable legal foundation for holding Gen-AI actors accountable, the actual enforcement requires careful judicial restraint and perhaps subsequent legislative clarity.

[28] Ibid
[29] Ibid

VI. SUGGESTIONS AND RECOMMENDATIONS- WHAT TO LEGISLATE ON GENERATIVE AI

Gen-AI's capacity to bypass human effort and cause instantaneous, large-scale harm mandates a regulatory framework that is both proactive and jurisprudentially precise. Despite *Kaushal Kishor* judgement, the foundation of remedies for violations remains structurally unsound without legislative or judicial clarity on three core issues, i.e., Defining the defendant, Establishing the chain of causation, and providing adequate remedies. Therefore, future regulation must primarily focus on equipping the judiciary, specifically the writ jurisdiction under Articles 32 and 226 to handle these techno-legal complexities.

The core challenge remains bringing large, powerful Gen-AI developers under the ambit of the 'State' defined in Article 12, thereby ensuring direct amenability to writ jurisdiction for fundamental rights violations. While *Kaushal Kishor* circumvented a strict Article 12 test by affirming horizontal rights, writ petitions against private entities still face resistance. We must evaluate whether private entities, due to the functional sovereignty they exert over vast swathes of public discourse, data, and access to essential knowledge, can be judicially deemed an 'instrumentality of the State' for specific constitutional purposes.

When a handful of LLM providers effectively determine what information is accessible or what narratives are amplified, they perform functions closely related to governmental or public importance. Legislation can either formally expand the definition of 'State' to include entities meeting a "public function/deep impact" test in the digital sphere, or the Judiciary, leveraging its inherent dynamism, can apply an expanded understanding of Article 12 to Gen-AI gatekeepers on a case-by-case basis.

The second, and perhaps most immediate, legislative imperative is solving the "chain of causation" problem. Usually, the aggrieved party must establish fault and a clear link between the defendant's action (or code) and the injury (e.g., deepfake harm, discriminatory output). Gen-AI's "black box" opacity and the involvement of multiple

actors (*data scraper, model developer, platform, user*) make this chain impossible to prove for the victim.[30]

In light of comparative developments within the European Union, particularly the Artificial Intelligence Act (Regulation (EU) 2024/1689) and the revised Product Liability Directive, 2024, Indian law must introduce a rebuttable presumption of causality for high-risk Gen-AI systems. Notably, the previously proposed EU AI Liability Directive has been formally withdrawn in October 2025, necessitating reliance on existing binding frameworks. This shifts the evidential burden: the Gen-AI developer must prove they were not at fault and adhered to strict safety and data governance standards, rather than the victim having to debug the AI's internal processes.

Furthermore, to provide comprehensive remedy for egregious violations of dignity and privacy under Article 21, the judiciary should actively recognize and refine a constitutional tort of AI-based reckless negligence. This would permit the courts to award punitive public law compensation against Gen-AI corporations for fundamental rights breaches, providing a quick, powerful redressal mechanism distinct from traditional civil suits. This blended approach of judicial creativity underpinned by targeted legislation is essential to translate the promise of Kaushal Kishor into practical accountability in the age of generative AI.

VII. CONCLUSION

The advent of Generative AI has exposed a critical constitutional accountability gap, where immense economic and social power concentrated in private corporate hands escapes the traditional, vertical constraints of fundamental rights jurisprudence. This article has demonstrated that Gen-AI's unique characteristics i.e., the opaqueness of its systems, the massive scale of its data scraping, and its capacity to cause non-physical, yet profound, harms like deepfake-based character assassination or systemic algorithmic discrimination render common law remedies insufficient. While the

[30] Kalagi, Sunil & Gubbewad, Renuka & Gondale, Aayush. (2024). LEGAL LIABILITIES OF ARTIFICIAL INTELLIGENCE: AN OVERVIEW. Journal of Law and Sustainable Development. 12. e3861. 10.55908/sdgs. v12i8.3861.

Supreme Court's declaration in *Kaushal Kishor v. State of U.P.* that Articles 19 and 21 have horizontal application is a jurisprudentially indispensable first step, its immediate practical utility is severely limited by the "black box" of causation and the narrow scope of Article 12. Therefore, to ensure that the constitutional promise of life and dignity extends fully into the digital sphere, the legal framework must be actively reconstructed.

The required reconstruction involves a dual mandate for both the legislature and the judiciary. The legislature must create robust mechanisms, such as mandating the rebuttable presumption of causality for high-risk AI systems, to alleviate the impossible burden of proof placed on the victim. Concurrently, the Indian Judiciary must engage in the necessary judicial creativity to bridge the definitional gaps. This means recognizing the functional sovereignty of powerful LLM providers, bringing them under an expanded constitutional discipline, and actively developing a constitutional tort of AI-based negligence to grant immediate and punitive public law compensation. Ultimately, securing fundamental rights against the unprecedented power of Gen-AI does not require constitutional amendment, but rather the timely and dynamic interpretation of existing principles, allowing the Constitution to remain a living document capable of guaranteeing Dignity and Equality in the age of algorithmic creation.

VIII. REFERENCES

1. Bordas et al, 'WHAT IS GENERATIVE IN GENERATIVE ARTIFICIAL INTELLIGENCE? A DESIGN-BASED PERSPECTIVE' (2024) 35 Research in Engineering Design 427
2. J. Euchner, 'Generative AI' (2023) 66(3) Research-Technology Management 71
3. F.J. García Peñalvo and A. Vázquez Ingelmo, 'WHAT DO WE MEAN BY GENAI? A SYSTEMATIC MAPPING OF THE EVOLUTION, TRENDS, AND TECHNIQUES INVOLVED IN GENERATIVE AI' (2023) 8(4) IJIMAI 7
4. S. Feuerriegel et al, 'Generative AI' (2024) 66 Business & Information Systems Engineering 111

5. Goldman Sachs, 'GENERATIVE AI COULD RAISE GLOBAL GDP BY 7%' (Goldman Sachs, 5 April 2023)
6. Kaushal Kishor v. State of U.P., (2023) 4 SCC 1
7. Emeka Duruigbo, 'Corporate Accountability and Liability for International Human Rights Abuses: Recent Changes and Recurring Challenges' (2008) 6(2) Northwestern Journal of International Human Rights
8. F. Pasquale, 'Two Visions for Data Governance: Territorial vs. Functional Sovereignty' in F. Pasquale (ed), Data Sovereignty (Oxford University Press 2023) 35.
9. Nikhil Narendran, 'A Case For Harmonizing Gen AI And The Copyright Regime' (Live Law, 24 Mar 2025) https://www.livelaw.in/articles/case-harmonizing-gen-ai-copyright-regime-287263
10. Rebecca Umbach, Nicola Henry, Gemma Faye Beard, and Colleen M. Berryessa. 2024. Non-Consensual Synthetic Intimate Imagery: Prevalence, Attitudes, and Knowledge in 10 Countries. In Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24), May 11--16, 2024, Honolulu, HI, USA
11. Bhattacharya, Saurav & Dodda, Suresh & Khanna, Anirudh & Panyam, Sriram & Balakrishnan, Anandaganesh & Jindal, Mayank. (2024). Generative AI Security: Protecting Users from Impersonation and Privacy Breaches. International Journal of Computer Trends and Technology. 72. 51-57. 10.14445/22312803/IJCTT-V72I4P106
12. Arijit Singh v. Codible Ventures LLP, 2024 SCC OnLine Bom 2445
13. Mustapha, Shehu & Man, Mustafa & Wan Abu Bakar, Wan Aezwani & Yusof, Kamir & ahmad sabri, Ily. (2024). Demystified Overview of Data Scraping. International Journal of Data Science and Advanced Analytics. 6. 290-296. 10.69511/ijdsaa. v6i6.205
14. Ryngaert, Cedric & Taylor, Mistale. (2020). The GDPR as Global Data Protection Regulation? AJIL Unbound. 114. 5-9. 10.1017/aju.2019.80.
15. Belenguer, Lorenzo. (2022). AI bias: exploring discriminatory algorithmic decision-making models and the application of possible machine-centric

solutions adapted from the pharmaceutical industry. AI and Ethics. 2. 771-787. 10.1007/s43681-022-00138-8

16. Kalagi, Sunil & Gubbewad, Renuka & Gondale, Aayush. (2024). LEGAL LIABILITIES OF ARTIFICIAL INTELLIGENCE: AN OVERVIEW. Journal of Law and Sustainable Development. 12. e3861. 10.55908/sdgs. v12i8.3861.