THE EXPANDING SCOPE OF ARTICLE 21: A CRITICAL ANALYSIS OF THE RIGHT TO PRIVACY, DIGITAL FREEDOMS AND CONSTITUTIONAL CHALLENGES POSED BY LARGE LANGUAGE MODELS (LLMs) IN INDIA

Jyotishman Thakuria, B.A. LL.B. (Hons.) NEF Law College, University of Gauhati, Guwahati

ABSTRACT

Article 21 of the Indian Constitution has never been static. It has evolved from a narrow procedural safeguard into one of the most powerful sources of substantive rights in Indian constitutional law. In the age of Artificial Intelligence (AI), particularly Large Language Models (LLMs) like ChatGPT, Claude, Gemini, Mistral, and DeepSeek, this evolution faces its most formidable constitutional test. These AI systems, trained on vast datasets often scraped without consent, directly challenge the right to informational privacy, digital freedoms, and human dignity, values that Article 21 is designed to protect.

This paper takes the position that existing jurisprudence, while flexible, is unprepared for the unique risks of generative AI. By examining landmark privacy judgments, the provisions of the Digital Personal Data Protection Act, 2023, and contrasting them with the European Union's AI regulatory approach, this paper argues that India's existing framework remains largely reactive, fragmented, and susceptible to excessive state intervention. The paper argues for a rights-based, anticipatory approach, one that embeds transparency, consent, and accountability into the very design and governance of LLMs. In doing so, the research bridges the gap between constitutional law and emerging technology, offering a pathway for India to craft a future-ready, rights-respecting AI governance model. Without such measures, Article 21 risks becoming a constitutional promise that technology can outpace and erode.

Keywords: Article 21; Right to Privacy; Digital Freedoms; Artificial Intelligence; Large Language Models; Generative AI; Data Protection; Constitutional Law; EU AI Act; DPDPA.

INTRODUCTION

Article 21 of the Indian Constitution, which declares that "No person shall be deprived of his life or personal liberty except according to procedure established by law", has consistently been recognised as one of the most dynamic and influential provisions within Indian Constitutional jurisprudence. Since its establishment, the understanding of Article 21 has changed significantly from being a limited procedural protection. The scope of Article 21 has grown by Indian Courts over time to encompass a broad range of fundamental rights required for a fulfilling and respectable life, including the right to privacy, access to clean air, legal assistance, shelter, and many more.[1]

Recent technological improvements have overtaken legal frameworks that have presented Article 21 with a whole new set of issues, one that is not related to the outdated legislation or traditional government overreach. The Indian constitutional framework is not entirely equipped to address the ethical and legal quandaries brought by the increasing use of Artificial Intelligence (AI) in our daily lives, especially through large language models (LLMs) like ChatGPT, Claude, Gemini, Mistral, and DeepSeek.

By analysing enormous volumes of textual data, LLMs, a class of Artificial Intelligence systems, are able to comprehend, produce, and work with language that is similar to that of human beings.[2] Built using deep learning architectures like transformers, these models, including ChatGPT, Claude, Gemini, Mistral, and DeepSeek, can generate text, respond to queries, create documents, and even mimic speech.[3]

Although LLMs offer a number of benefits, including enhancing educational delivery, expanding access to legal knowledge, and assisting in the provision of public services, they also bring up urgent issues with privacy, data governance, and algorithmic transparency. Without explicit responsibility or informed agreement, these systems are trained on enormous

[1] Maneka Gandhi v. Union of India (1978) 1 SCC 248; Francis Coralie Mullin v. Administrator, Union Territory of Delhi, (1981) 1 SCC 608.

[2] Tom B Brown et al., *Language Models Are Few-Shot Learners*, 33 ADVANCES IN NEURAL INFO. PROCESSING SYS. 1877 (2020) https://papers.nips.cc/paper_files/paper/2020/file/1457c0d6bfcb4967418bfb8ac142f64a-Paper.pdf (last visited July 1 2025).

[3]OpenAI, *Introducing ChatGPT,* OPENAI (Nov. 30, 2022) https://openai.com/blog/chatgpt (last visited July 1 2025); DeepSeek, *DeepSeek Chat,* DEEPSEEK (n.d.) https://chat.deepseek.com/ (last visited July 2 2025).

datasets that are frequently collected from public and semi-public digital areas.[4] Human dignity and informational privacy, two rights firmly rooted in Article 21, may be violated as a result.[5]

This research paper aims to critically assess whether the existing reading of Article 21 can adequately handle the new constitutional problems raised by generative AI tools such as LLMs. In order to comprehend how India's use and abuse of AI technologies affect fundamental rights, it focuses particularly on two pillars of Article 21, the right to privacy and digital freedoms. The research paper also investigates whether or not the judiciary can effectively guide the regulation of AI systems by analysing how it has interpreted ideas like accountability, transparency, and fairness, concepts that are not expressly mentioned in Article 21.[6]

This research paper aims to identify gaps, raise relevant constitutional issues, and provide a path forward, in addition to critiquing the existing jurisprudence.

In doing so, this paper not only examines the constitutional scope of Article 21 in the age of AI but also compares India's evolving digital governance framework with that of the European Union, ultimately advocating for the creation of a dedicated AI regulatory authority capable of safeguarding fundamental rights in an increasingly automated society.

LITERATURE REVIEW

Article 21 of the Indian Constitution has undergone a significant doctrinal evolution over time, transforming from a procedural safeguard to a foundation for substantive rights that are essential to human dignity. In *A.K. Gopalan v. State of Madras*,[7] the Supreme Court initially adopted a narrower interpretation, taking "procedure established by law" at face value and omitting due process. However, by integrating the concepts of justice, fairness, and reasonableness into Article 21, the landmark decision in *Maneka Gandhi v. Union of India*[8] significantly altered this position. This transformation has enabled the recognition of a wide array of rights, including the right to a dignified life, adequate housing, employment, education,

[4] Vidushi Marda, *Artificial Intelligence and the Right to Privacy in India*, (Data & Soc'y 2018) https://datasociety.net/library/artificial-intelligence-and-the-right-to-privacy-in-india/ (last visited July 2 2025).
[5] Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1(India).
[6] State of Punjab v. Gurdev Singh (1991) 4 SCC 1; Shreya Singhal v. Union of India (2015) 5 SCC 1; Anuradha Bhasin v. Union of India (2020) 3 SCC 637.
[7] A.K. Gopalan v. State of Madras AIR 1950 SC 27.
[8] Maneka Gandhi v. Union of India (1978) 1 SCC 248.

and access to legal support, among others.[9]

In *Francis Coralie Mullin v. Administrator, Union Territory of Delhi*,[10] the court expanded the scope of the right to life, holding that it encompasses more than mere animal existence. Similarly, in *Olga Tellis v. Bombay Municipal Corporation*,[11] the right to livelihood was read as an integral component of the right to life under Article 21. These cases form the bedrock of modern constitutional interpretation of the right to life.

The jurisprudential shift reached its most significant turning point with the unanimous nine-judge bench decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India*,[12] which declares the right to privacy as intrinsic to Article 21. The judgment discussed informational self-determination, bodily integrity, and decisional autonomy. It cited both Indian and comparative constitutional law, including privacy protections under the American and European systems. The judgment emphasised that privacy is not an elitist construct but a condition for freedom and dignity.

Legal scholars like **Gautam Bhatia** in *The Transformative Constitution*[13] and **Suhrith Parthasarathy,** in journal articles[14], have argued that the right to privacy, as a fundamental right, must be robust enough to evolve with technology. These ideas are echoed in works like **Rohit De's** historical analysis of how constitutional rights have expanded through everyday litigation,[15] and in **Tarunabh Khaitan's** theoretical writings on dignity jurisprudence, which underpins privacy as recognised in Indian constitutional law[16].

Alongside the right to privacy, digital freedoms have increasingly drawn judicial attention. In *Shreya Singhal v. Union of India*,[17] the Supreme Court invalidated Section 66A of the Information Technology Act, 2000, on the ground that it imposed unconstitutional restrictions

[9] Mohini Jain v State of Karnataka (1992) 3 SCC 666; Unni Krishnan v State of Andhra Pradesh (1993) 1 SCC 645.
[10] Francis Coralie Mullin v. Administrator, Union Territory of Delhi (1981) 1 SCC 608.
[11] Olga Tellis v. Bombay Municipal Corporation (1985) 3 SCC 545.
[12] Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1.
[13] GAUTAM BHATIA, THE TRANSFORMATIVE CONSTITUTION: A RADICAL BIOGRAPHY IN NINE ACTS (HarperCollins Publishers 2019).
[14] Suhrith Parthasarathy, *A Common Law of Privacy for India*, 129 YALE L.J.F. 147 (2019).
[15] ROHIT DE, A PEOPLE'S CONSTITUTION: THE EVERYDAY LIFE OF LAW IN THE INDIAN REPUBLIC (Princeton Univ. 2018).
[16] Tarunabh Khaitan, *Dignity as an Expressive Norm: Neither Vacuous Nor a Panacea*, 32 OXFORD J. LEGAL STUD. 1 (2012).
[17] Shreya Singhal v. Union of India (2015) 5 SCC 1.

on online free expression. Similarly, in *Anuradha Bhasin v. Union of India*[18] the court established procedural safeguards to protect internet access, recognising its significance for both free speech and the right to carry on trade.

Despite these important steps, Indian jurisprudence remains relatively silent on algorithmic governance, especially involving generative AI models like ChatGPT and DeepSeek. These large language models (LLMs) are a subset of artificial intelligence capable of generating human-like text based on training on massive datasets.[19] While AI has been discussed in Indian policy circles, particularly in the Justice B.N. Srikrishna Committee Report on data protection,[20] there has been no clear judicial stance on its constitutional impact.

Scholars such as **Vidushi Marda** have warned against the opaque nature of algorithmic decision-making and its threat to privacy. Her article, *Artificial Intelligence and the Right to Privacy in India*,[21] argues that unless the Indian legal system adopts accountability and transparency measures, the unchecked deployment of AI will erode fundamental rights. Organisations like the Software Freedom Law Centre have documented the proliferation of AI-enabled surveillance through facial recognition technologies and the lack of safeguards for privacy and civil liabilities.[22]

Globally, the UNESCO Recommendation on the Ethics of AI[23] and OECD Principles on Artificial Intelligence[24] have attempted to introduce a rights-based, ethical AI governance framework. These guidelines emphasised transparency, fairness and human oversight, values already read into Article 21 by Indian courts. However, these frameworks remain aspirational in India, with no binding regulatory framework in place.

Technical literature such as the paper Language Models are Few-Shot Learners[25] by Brown et

[18] Anuradha Bhasin v. Union of India (2020) 3 SCC 637.
[19] Brown et al., supra note 2.
[20] Justice B.N. Srikrishna Comm., *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, (Ministry of Electronics & Info. Tech., July 2018), https://www.naavi.org/uploads_wp/new/Data_Protection_Committee_Report.pdf (last visited July 3 2025).
[21] Vidushi Marda., supra note 4.
[22] Software Freedom Law Ctr., *India, Analysis of the Facial Recognition Technology-Enabled Surveillance Landscape in India* (Jan. 16, 2024), https://sflc.in/analysis-of-the-facial-recognition-technology-enabled-surveillance-landscape-in-india/ (last visited July 5 2025).
[23] UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021), https://unesdoc.unesco.org/ark:/48223/pf0000381137 (last visited July 5 2025).
[24] OECD, *Recommendation of the Council on Artificial Intelligence* (OECD Legal Instrument No 0449, 2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (last visited July 7 2025).
[25] Brown et al., supra note 2.

al., explore the scale and functioning of LLMs, but there's a stark absence of constitutional scholarship examining how such models intersect with Indian fundamental rights. This paper aims to fill that gap by critically analysing whether the interpretive boundaries of Article 21 can meaningfully accommodate and regulate the constitutional risks posed by generative AI.

While existing scholarship has thoroughly explored the contours of Article 21 in the context of privacy, free speech, and informational autonomy, there remains a notable gap in the analysis of large language models (LLMs) such as ChatGPT, DeepSeek, Gemini, and Claude, and their unique constitutional implications. Academic literature in India has primarily examined AI in broad terms, often without focusing on the distinct risks posed by generative AI systems, such as deepfake creation, misinformation, and bias in automated decision-making.[26] Moreover, comparative perspectives on how other jurisdictions, particularly the European Union under the GDPR and the AI Act, address these challenges are sparse.[27] This paper seeks to fill these gaps by integrating doctrinal analysis with real-world examples and a comparative study, ultimately advocating for the establishment of a dedicated AI regulatory authority to ensure that technological progress is balanced with the protection of fundamental rights under Article 21.

THE EXPANDING CONSTITUTIONAL SCOPE OF ARTICLE 21

1) The Expanding Interpretation of Article 21:

The Indian Constitution, under Article 21, states that, "No person shall be deprived of his life or personal liberty except according to procedure established by law". At first glance, this provision appears procedural, but over the years, it has emerged as one of the most powerful sources of substantive rights in Indian constitutional law. In *A.K. Gopalan v. State of Madras* (1950), Article 21 was initially given a restrictive interpretation, limited to procedural legality.[28] This narrow approach was later overturned in *Maneka Gandhi v. Union of India* (1978), where the Supreme Court ruled that any procedure restricting life or personal liberty must be "just,

[26] NITI Aayog, *National Strategy for Artificial Intelligence: Discussion Paper* (2018), https://www.niti.gov.in/sites/default/files/2019-01/NationalStrategy-for-AI-Discussion-Paper.pdf (last visited July 20 2025).

[27] European Commission, *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence,* COM (2021) 206 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 (last visited July 20 2025).

[28] A.K. Gopalan v. State of Madras AIR 1950 SC 27.

fair, and reasonable."[29] The judgment marked a transformative shift, laying the foundation for a broader and more substantive understanding of the right to life and personal liberty.

Following Maneka Gandhi, the Supreme Court has recognised a range of unenumerated rights within the ambit of Article 21, including the right to live with dignity and the right to livelihood in *Olga Tellis v. Bombay Municipal Corporation*,[30] and the right to shelter, as an outcome of *Shantistar Builders v. Narayan Khimala Totame*,[31] and the right to health in *Paschim Banga Khet Mazdoor Samity v. State of West Bengal*.[32] Collectively, these rulings illustrate a progressive judicial trend that aligns constitutional interpretation with the practical realities of Indian citizens' lives.

2) Judicial Recognition of the Right to Privacy:

The recognition of the right to privacy as a fundamental right marked an important moment in Indian constitutional jurisprudence. In Justice *K.S. Puttaswamy (Retd.) v. Union of India* (2017), a nine-judge bench unanimously affirmed that privacy is intrinsic to life and liberty under Article 21.[33] The Court articulated a three-pronged test to determine the constitutionality of any infringement of privacy:

- Legality: Existence of a valid law.
- Necessity: In relation to a legitimate state aim.
- Proportionality: A rational nexus between the means adopted and the objective sought to be achieved.

The judgment identified various facets of privacy, including bodily integrity, informational privacy, and decisional autonomy. Of particular relevance to this paper is the notion of informational privacy, which concerns a person's right to control the use and dissemination of personal data. In today's digital landscape, this aspect of privacy assumes heightened importance.

[29] Maneka Gandhi v. Union of India (1978) 1 SCC 248.
[30] Olga Tellis v. Bombay Municipal Corporation (1985) 3 SCC 545.
[31] Shantistar Builders v. Narayan Khimala Totame (1990) 1 SCC 520.
[32] Paschim Banga Khet Mazdoor Samity v. State of West Bengal (1996) 4 SCC 37.
[33] Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1.

3) Article 21 in the Digital Era:

The digital age has transformed how we communicate, transact, and engage with the world, making digital freedoms a crucial extension of traditional constitutional rights. The judiciary has acknowledged this transition in several cases. In *Shreya Singhal v. Union of India* (2015), the court struck down Section 66A[34] of the Information Technology Act for violating the freedom of speech and expression.[35] In *Anuradha Bhasin v. Union of India* (2020), the Supreme Court recognised internet access as essential for the exercise of fundamental rights.[36]

Similarly, in *Faheema Shirin v. State of Kerala*, the Kerala High Court held that access to the internet forms an integral part of the right to education, and by extension, the rights to privacy and dignity under Article 21.[37] Together, these decisions reflect a judicial openness to extending constitutional rights into the digital sphere, albeit in a manner that remains largely reactive rather than anticipatory.

4) Constitutional Challenges Posed by Large Language Models (LLMs):

This paper specifically explores how large language models (LLMs), such as ChatGPT, Claude, Gemini, Mistral, and DeepSeek, raises novel constitutional challenges under Article 21. These AI systems are trained on massive datasets, some of which may include publicly available personal data. The training process itself lacks transparency, and users whose data may be scraped and used are rarely informed, let alone asked for consent.

Some of the popular LLMs are:

- ChatGPT, developed by OpenAI, is a conversational LLM capable of generating human-like text based on user prompts.[38]

- Claude, developed by Anthropic, emphasises safety and alignment with human values and is particularly designed for responsible use.[39]

[34] Information Technology Act, No. 21 of 2000, § 66A (India) (Struck down).
[35] Shreya Singhal v. Union of India (2015) 5 SCC 1.
[36] Anuradha Bhasin v. Union of India (2020) 3 SCC 637.
[37] Faheema Shirin v. State of Kerala 2019 SCC OnLine Ker 3150.
[38] OpenAI, *ChatGPT*, OPENAI (n.d.) https://openai.com/chatgpt (last visited July 8 2025).
[39] Anthropic, *Claude,* ANTHROPIC (2023) https://www.anthropic.com/claude (last visited July 8 2025).

- Google's Gemini, formerly known as Bard, integrates multimodal capabilities such as text, image, and code understanding.[40]

- Mistral is a French open-weight model built for transparency and fine-tuning across varied use cases.[41]

- DeepSeek is a multilingual LLM with a focus on legal and academic contexts, known for its ability to search and synthesise across multiple sources.[42]

Each of these models operates differently in terms of training, alignment, and data policies, yet all pose questions about data provenance, informed consent, and misuse.

From the perspective of informational privacy, large language models (LLMs) pose a significant challenge to the foundational principles established in the *Puttaswamy* judgment. The expectation that individuals should have control over their personal information is incompatible with the opaque data ingestion practices of LLMs. If an LLM is trained on user-generated data without consent and reproduces sensitive or identifying information, it may infringe the right to informational privacy. Moreover, the use of LLMs by governmental entities, educational institutions, and digital public platforms must meet the *Puttaswamy* test. Presently, India does not have a comprehensive data protection law in force, making it difficult to establish the legality of such practices. Even if a legitimate aim, such as improving efficiency in public services, exists, the deployment of such AI tools must be proportionate and accompanied by safeguards.

LLMs also pose the risk of profiling, algorithmic bias, and misinformation. These outputs can affect the dignity and autonomy of individuals, values central to Article 21. The black-box nature of these systems makes it harder to ensure accountability, creating a potential for untraceable harm.[43]

5) Doctrinal Gaps and the Need for Reform:

Despite the broad interpretations of Article 21, Indian jurisprudence has not yet adequately

[40] Google DeepMind, *Gemini*, GOOGLE DEEPMIND (2023) https://deepmind.google/technologies/gemini/ (last visited July 8 2025).
[41] Mistral AI, *Mistral AI,* MISTRALAI (n.d.) https://mistral.ai (last visited July 9 2025).
[42] DeepSeek, *DeepSeek Chat,* DEEPSEEK (n.d.) https://chat.deepseek.com/ (last visited July 9 2025).
[43] Vidushi Marda, supra note 4.

responded to the constitutional implications of LLMs. While existing doctrines provide a strong foundation, there is a need for courts to explicitly address how new technologies affect privacy, autonomy, and dignity.

This paper contends that the judiciary should adopt a forward-looking interpretive approach, one that not only applies existing privacy tests to AI but also calls for legislative clarity and technological accountability. Until comprehensive data protection and AI governance frameworks are enacted, the constitutional promises of Article 21 remain under threat in the age of generative AI.

This analysis serves to bridge the doctrinal gap and urges both judicial and legislative institutions to adopt constitutional protections in the rapidly changing digital environment.

6) Digital Personal Data Protection Act, 2023:

The Digital Personal Data Protection Act, 2023 (DPDPA), emerged as a legislative response to the Supreme Court's landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*,[44] which unequivocally affirmed the right to privacy as a fundamental right under the Constitution. As India's first comprehensive data protection law, the DPDPA establishes a framework for safeguarding individual privacy, extending its scope to personal data processed in digital form as well as non-digital data that is intended for digitisation and subsequent processing.[45] It mandates entities collecting and processing personal data, Data Fiduciaries, to adhere to core principles such as obtaining free, specific, informed and unambiguous consent, with limited data expectations for legitimate uses, ensuring lawful and fair processing, limiting data collection to what is necessary for the stated purpose, maintaining data accuracy, implementing robust security safeguards to prevent breaches,[46] and notifying the Data Protection Board of India (DPBI) and affected individuals in case of significant breaches.[47] The Act grants individuals, Data Principals, significant rights over their data, including the right to access, correct, erase, update, and seek grievance redressal.[48] It establishes the DPBI as the regulatory authority, introduces the concept of "Consent Managers" to facilitate consent,

[44] Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1.
[45] Digital Personal Data Protection Act, No. 22 of 2023, §§ 4–6 (India).
[46] Id. §§ 7–9.
[47] Id. §§ 10–12.
[48] Id. §§ 13–15.

sets out penalties for non-compliance, and provides rules for cross-border data transfers.[49]

Despite its significance, the Digital Personal Data Protection Act, 2023, has critical gaps when examined through the lens of large language models (LLMs) and emerging AI technologies. One of the major issues is the Act's lack of AI-specific provisions. While it provides a general framework for data protection, it does not address the unique challenges posed by LLMs, such as the use of scraped data from open sources, the generation of synthetic data that mimics real individuals, and the difficulty in tracing data origin within large models.

Further, the Act lacks transparency and accountability mandates for AI developers. LLMs operate an opaque system, often termed 'Black Boxes', which means that users have little clarity on what data is used, how it is processed, or whether their personal data contributed to the model's training. The DPDPA does not require disclosure of training datasets, nor does it mandate impact assessments or algorithmic audits that could prevent misuse or bias.

Another major shortcoming is the Act's broad exemptions for the state. The government may be exempted from several provisions on grounds of national interest, public order, or security, potentially opening the door for mass surveillance or unregulated state use of LLMs without constitutional safeguards. Moreover, the Act is silent on profiling, automated decision-making, and algorithmic discrimination, core concerns in the context of generative AI. This leaves individuals vulnerable to being affected by biased or harmful outputs generated by LLMs, without any meaningful legal recourse.

Lastly, while DPDPA lays down the groundwork for digital privacy, it falls short of addressing the evolving risks of LLMs and urgently needs AI-specific amendments and/or complementary legislation.

REAL-WORLD IMPLICATIONS OF LLM MISUSE:

The increasing deployment of large language models (LLMs) like ChatGPT, Claude, Gemini, DeepSeek, and others has already triggered several real-world incidents that highlight the constitutional challenges they pose, particularly in relation to privacy, informational autonomy, and digital dignity under Article 21.

[49] Id. §§ 16–18.

1. One of the most concerning incidents was the ChatGPT data leak in March 2023. Due to a vulnerability in the open-source library *redis-py,* a bug briefly exposed the chat histories and payment information of users, including email addresses and the last four digits of credit card numbers. This incident revealed how fragile users' privacy can be in AI-driven platforms, undermining the expectations of confidentiality and violating principles of informational privacy.[50]

2. Another concerning issue is the presence of algorithmic bias. Research by the Centre for Democratic & Technology highlights that generative AI systems often reinforce harmful stereotypes and reflect existing societal prejudices. For example, large language models may generate outputs that perpetuate gendered or racialised assumptions, demonstrating how underlying biases in training data manifest in discriminatory results.[51] Such discriminatory outputs threaten the dignity and equality of individuals and could potentially violate constitutional protections under Article 14 and Article 21.

3. Moreover, LLMs are increasingly being used in the creation of deepfake-style misinformation. Reports have shown how generative text models have been exploited to mass-produce fabricated news articles and misleading narratives, raising concerns about defamation, identity misuse, and manipulation of public discourse.[52]

4. One other troubling dimension is the use of AI-powered deepfakes in financial fraud. In one notable case, employees of the UK engineering firm Arup were deceived into transferring approximately $25 million after participating in a video call where fraudsters used deepfake technology to impersonate senior executives. This single instance reflects a broader global trend, where deepfake scams have surged, causing over $200 million in reported financial losses within a quarter.[53]

---

[50] Jon Porter, *ChatGPT bug temporarily exposes AI chat histories to other users*, THE VERGE (21 Mar. 2023), https://www.theverge.com/2023/3/21/23649806/chatgpt-chat-histories-bug-exposed-disabled-outage (last visited July 11 2025).

[51] Hannah Quay-de la Vallee, *Generative AI Systems in Education – Uses and Misuses,* CTR. FOR DEMOCRACY & TECH. (15 Mar., 2023), https://cdt.org/insights/generative-ai-systems-in-education-uses-and-misuses/ (last visited July 11 2025).

[52] Matthew Gault, *AI Spam Is Already Flooding the Internet and It Has an Obvious Tell*, VICE (24 Apr., 2023), https://www.vice.com/en/article/ai-spam-is-already-flooding-the-internet-and-it-has-an-obvious-tell (last visited July 12 2025).

[53] Angus Loten, *AI Drives Rise in CEO Impersonator Scams,* WALL ST. J. (18 Aug. 2025), https://www.wsj.com/articles/ai-drives-rise-in-ceo-impersonator-scams-2bd675c4 (last visited Aug. 19 2025).

5. The misuse of LLMs is not confined to financial fraud. Platforms integrating AI chatbots have seen concerning ethical lapses. Meta's internal policy documents revealed that its chatbots were at times allowed to generate inappropriate interactions with minors, dispense inaccurate medical information, and even produce harmful or discriminatory outputs.[54]

6. Privacy concerns are also amplified by recent LLM capabilities. ChatGPT's image reasoning tools have been used to conduct "reverse location searches", identifying where personal photos were taken even in the absence of metadata. This function, while technologically impressive, risks enabling stalking, doxing, and unlawful surveillance.[55]

7. India has already witnessed direct social harm from deepfake misuse. In a widely publicised case, influencer Archita Phukan (popularly known as "Babydoll Archi") was victimised through an AI-generated pornographic deepfake. The perpetrator, her former partner, monetised the content and earned significant profits while defaming her image. The case reflects not only personal harm but also a glaring gap in India's ability to address gendered harms caused by AI technologies.[56]

8. The use of web scraping by AI developers without user consent is another concern. LLMs like GPT-3.5 and Claude are often trained on vast datasets scraped from websites, blogs, social media, and forums, without informing the content creators or obtaining valid consent. This concern is highlighted in Google's own admission that its LLM Bard relies on publicly available data scraped from the web, raising questions about transparency and consent in AI training practices.[57] This practice conflicts with the consent principle upheld in Puttaswamy and also appears to fall outside the intended safeguards of the

[54] Jeff Horwitz, *Meta's AI Rules Have Let Bots Hold "Sensual" Chats with Kids, Offer False Medical Info*., REUTERS (14 Aug. 2025), https://www.reuters.com/business/metas-ai-rules-have-let-bots-hold-sensual-chats-with-kids-offer-false-medical-2025-08-14 (last visited Aug. 17 2025).

[55] Chiara Castro, Beware, *Another ChatGPT Trend Threatens Your Privacy – here's how to stay safe*, TECHRADAR (25 Apr. 2025), https://www.techradar.com/computing/cyber-security/beware-another-chatgpt-trend-threatens-your-privacy-heres-how-to-stay-safe (last visited Aug. 17 2025).

[56] Nancy Jaiswal, *Babydoll Archi's ex-boyfriend turns revenge into AI racket, earns money by faking influencer's identity online*, INDIA TIMES (14 July 2025), https://indiatimes.com/trending/babydoll-archi-dragged-into-ai-porn-storm-ex-boyfriends-deepfake-scam-exposed-crores-earned-with-fake-nude-content-663824.html (last visited Aug. 18 2025).

[57] Jess Weatherbed, *Google confirms it's training Bard on scraped web data, too*, THE VERGE (5 July 2023), https://www.theverge.com/2023/7/5/23784257/google-ai-bard-privacy-policy-train-web-scraping (last visited July 15 2025).

Digital Personal Data Protection Act, 2023.

9. There have even been instances of AI being misused to impersonate legal professionals. In 2023, a fake "AI lawyer" bot was found offering legal advice on social media platforms while presenting itself as being affiliated with a real law firm. The content it produced was misleading and potentially harmful. The lack of accountability and verifiability in such impersonation cases calls into question the adequacy of current regulatory tools to preserve the sanctity of the legal profession and protect citizens from misrepresentation.

These examples underscore the urgent need for a robust regulatory and constitutional framework to govern the development and deployment of LLMs in India. They highlight how current laws, including the DPDPA, may be insufficient in addressing the nuanced and rapidly evolving challenges posed by AI technologies.

COMPARATIVE ANALYSIS: INDIAN AND EUROPEAN APPROACHES TO REGULATING LLMS:

The regulation of large language models (LLMs) has taken divergent paths globally. While India is in the early stages of framing comprehensive policies to govern artificial intelligence and data-driven technologies, the European Union (EU) has been more proactive and structured in its regulatory response. This section provides a comparative analysis of the regulatory frameworks in India and the European Union, particularly focusing on the EU AI Act, the General Data Protection Regulation (GDPR), and India's Digital Personal Data Protection Act, (DPDPA). This comparison highlights critical gaps, strengths, and lessons that India may consider to ensure that its constitutional promise under Article 21 is effectively protected in the era of artificial intelligence.

1. The EU AI Act: In March 2024, the European Union enacted the AI Act, establishing the world's first comprehensive legal framework for regulating artificial intelligence, including large language models. The Act employs a risk-based classification, dividing AI systems into categories of unacceptable, high, limited, and minimal risk. High-risk applications, such as biometric identification and predictive policing, are subject to stringent compliance obligations relating to transparency, data governance, human

oversight, and accountability.[58]

While the Act does not name specific LLMs, it classifies general-purpose AI models with significant impact as "systemic", requiring regular assessments and disclosures about training data, performance, and risk mitigation. This is highly relevant in the context of models like ChatGPT, which generate content at scale and influence user behaviour, decisions, and access to information.[59]

2. GDPR and the Emphasis on Data Protection: The General Data Protection Regulation (GDPR), enforced since 2018, lays a strong foundation for personal data protection in the EU. It mandates lawful processing of data, user consent, and the right to be forgotten, and imposes heavy penalties for violations. Significantly, Article 22 of the GDPR grants individuals the right not to be subjected to decisions based exclusively on automated processing, including profiling, where such decisions produce legal consequences or similarly significant effects.[60]

   This provision creates an implicit regulatory control over LLMs, especially those used in recruitment, credit scoring, or content moderation. Moreover, GDPR's insistence on data minimisation and purpose limitation sharply contrasts with the opaque data-collection practices of many commercial LLMs.

3. India's Digital Personal Data Protection Act, 2023: India's Digital Personal Data Protection Act (DPDPA), 2023, adopts a more sectoral and flexible approach to data regulation. The statute introduces concepts such as 'data fiduciaries', user consent requirements, and audit provisions similar to those found in the GDPR. However, while it provides a framework for safeguarding personal data, it does not address AI-specific

[58] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] O.J. L 202/1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689 (last visited July 15 2025).

[59] European Parliament, *EU AI Act: first regulation on artificial intelligence,* EUROPEAN PARLIAMENT (8 June 2023, updated 19 Feb. 2025), https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (last visited July 15 2025).

[60] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, [2016] O.J. L 119/1 (General Data Protection Regulation).

risks such as algorithmic bias, model explainability, and autonomous decision-making.

Further, the DPDPA gives considerable discretion to the central government to exempt certain government agencies from its provisions, raising concerns about surveillance and misuse of data, thus potentially undermining privacy rights under Article 21.[61]

4. Key Differences and Constitutional Implications: Some of the main differences between the Indian and the European Union's approach towards LLMs are –

    - The European Union, by the implementation of the AI Act, 2024, have AI-specific laws, whereas there is no AI-specific legislation in India yet.

    - The European Union have stronger, detailed provisions for data protection through GDPR, while India, comparatively, has a basic framework for data protection through DPDPA.

    - In the European Union, transparency requirements for LLMs are mandatory for systematic models. But no such requirement is mentioned in any of India's legislation.

    - Article 22 of the GDPR explicitly covers automated decision-making regulation, but the same is not addressed for India.

    - For any redressal and enforcement regarding any violation of the provisions, the European Union have independent regulators and violators are awarded with high penalties. In India, the same is enforced by a government-appointed Board and has limited teeth.

    - The European Union's AI-specific laws are highly aligned with fundamental rights, whereas in India, it is moderately aligned, and the government has overriding powers.

[61] Rahul Matthan, *Get on with data protection now that the law's enacted*, MINT (15 Aug. 2023), https://www.livemint.com/opinion/online-views/get-on-with-data-protection-now-that-the-law-s-enacted-11692108114742.html (last visited July 17 2025); Digital Personal Data Protection Act, No. 22 of 2023, § 17(2) (India).

- The European model better aligns with fundamental rights jurisprudence, ensuring transparency, proportionality, and accountability. In India, while judicial interpretation of Article 21 has recognised the right to privacy, legislative efforts like the DPDPA are yet to match the precision and enforceability seen in European instruments.

5. Importance of this comparison: For India to effectively regulate LLMs in a manner consistent with constitutional values, especially those under Article 21, it must transition from a reactive to a proactive regulatory posture. Lessons from Europe highlight the need for:

    - Mandatory transparency obligations on LLM developers,
    - Legal safeguards against algorithmic discrimination.
    - Independent and empowered oversight bodies,
    - Strict limitations on surveillance and data sharing.

Such measures would not only strengthen India's AI governance but also fulfil its constitutional commitment to uphold individual dignity, informational autonomy, and digital freedom in a rapidly evolving technological world.

SUGGESTIONS:

1) Comprehensive Data Protection Legislation: India must expedite the enactment of a robust data protection law aligned with international standards like the European Union's General Data Protection Regulation (GDPR), a detailed legislative framework that governs how organisations collect. The GDPR governs the use, storage, and transfer of personal data belonging to individuals in the European Union. Its primary objective is to enhance individual control over personal data while harmonising data protection standards across member states. Importantly, the regulation applies extraterritorially, extending to any organisation that processes the personal data of EU residents, irrespective of where the organisation is located.

   Such legislation should specifically address how AI and LLMs can collect, process, and

store personal data.

2) Judicial Interpretation of AI-Driven Violations: The Supreme Court and High Courts should take proactive steps to interpret constitutional protections in the context of emerging AI technologies. Judicial guidelines could define the threshold for consent, proportionality, and legality in the development of LLMs.

3) AI Ethics and Privacy Audit Framework: A national-level regulatory body should be established to audit LLMs used by public and private entities. These audits should assess models' training data, data privacy, and bias mitigation mechanisms.

4) Digital Literacy and Consent Awareness: The government should implement awareness programs focused on digital rights and data privacy, particularly in rural and underserved areas. Informed digital consent must become a constitutional norm, not a privilege.

5) Inclusion of AI Governance in Judicial Training: Judicial academies should introduce modules on AI, data privacy, and LLMs so that the judiciary is better equipped to deal with tech-related constitutional issues.

6) Transparent Use of LLMs in Public Sector: All government uses of LLMs, whether in education, administration, or legal services, should be subjected to public scrutiny, transparency obligations, and human oversight.

7) AI Specific Amendments to the Digital Personal Data Protection Act, 2023: While the DPDPA provides a foundational framework for data privacy, it lacks provisions tailored to the regulation of artificial intelligence systems, particularly Large Language Models. The Act should be amended to include AI-specific safeguards such as mandatory algorithmic audits, transparency in training datasets, and clear redress mechanisms for harm caused by automated decision-making. It should also require developers of LLMs to disclose data provenance and implement fairness assessments to prevent bias or discrimination.

   These amendments would align the DPDPA with the evolving nature of data-driven technologies and reinforce constitutional protections under Article 21.

8) Adopt Best Practices from the EU AI Act and GDPR: India's AI governance framework can draw on the EU's risk-based classification of AI systems, mandatory transparency

disclosures for general-purpose AI, and strong individual rights protections under GDPR, adapted to the Indian constitutional framework to ensure enforceability and proportionality.[62]

CONCLUSION:

The evolution of Article 21 of the Indian Constitution from a procedural safeguard to a robust source of substantive rights has been one of the most transformative developments in Indian constitutional law. Over the decades, judicial interpretations have extended its scope to encompass a wide array of human rights, including the right to privacy, dignity, autonomy, and more recently, digital freedoms. This paper has sought to contextualise these developments in light of the rise of large language models (LLMs) such as ChatGPT, Claude, Gemini, Mistral, and DeepSeek and the constitutional challenges they present in a digital society.

The Supreme Court's decision in Justice *K.S. Puttaswamy (Retd.) v. Union of India* marked a transformative moment in the interpretation of Article 21, firmly establishing the right to privacy as a fundamental constitutional guarantee, particularly in a digital era dominated by data-driven technologies. Yet, the advent of large language models (LLMs) presents novel challenges that the existing legal framework has not fully anticipated. These systems rely on complex algorithms trained on vast datasets, often without meaningful user consent. Such opacity directly threatens the constitutional guarantee of informational privacy, an essential component of Article 21.

While courts have shown a commendable willingness to protect digital freedoms, such as in Shreya Singhal and Anuradha Bhasin cases, their responses remain largely reactive. What is required is a forward-looking judicial approach that can anticipate technological developments and ensure that constitutional safeguards evolve accordingly. The proportionality test articulated in the *Puttaswamy* judgment, comprising legality, necessity, and proportionality, requires reassessment and refinement in the light of the emergence of large language models and artificial intelligence more broadly.

The introduction of the Digital Personal Data Protection Act, 2023, is a commendable legislative development that codifies critical principles of informational privacy. It also

[62] European Parliament, supra note 59.

establishes a framework for grievance redressal and user empowerment. However, its silence on issues specific to AI, like algorithmic transparency, dataset disclosures, or profiling safeguards, underscores the urgent need for targeted amendments. Integrating AI-specific obligations into the statute would ensure a robust legal foundation for regulating LLMs and other generative technologies.

This paper advocates for the creation of AI-specific legal standards, including doctrines on data provenance, algorithmic transparency, and explainability. These principles would enable courts and regulators to better evaluate the legality and impact of AI tools on citizens' rights.

A key recommendation emerging from this study is the establishment of a dedicated AI regulatory authority with the power to oversee LLM development, enforce algorithmic transparency, mandate bias audits, and provide accessible redressal mechanisms. Without such an institution, India risks allowing private actors and foreign platforms to shape the boundaries of its citizens' fundamental rights.

In essence, Article 21 stands as a testament to the dynamic and evolving nature of the Indian Constitution. As LLMs become more integrated into governance and daily life, it is imperative to reaffirm the values enshrined in this article. Only then can we ensure that constitutional protections remain robust and relevant in the age of artificial intelligence.