SvedbergOpen
DISSEMINATION OF KNOWLEDGE
International Journal of Artificial Intelligence and Machine Learning
Publisher's Home Page: https://www.svedbergopen.com/
Research Paper Open Access

Judging AI: Lessons For India From USA And EU

Dr. Arjun Philip George[1*], Sahaya Trinity[2]

[1*]Assistant Professor (Sr.), Vellore Institute of Technology, School of Law, Vellore Institute of Technology, Chennai, Tamil Nadu 600127, India. Email: arjunphilip.george@vit.ac.in
[2]BBA LLB (Hons.) Student, Vellore Institute of Technology, School of Law,
Vellore Institute of Technology, Chennai, Tamil Nadu 600127, India. Email: sahaya.trinity2024@vitstudent.ac.in

Abstract. As the world enters Industry 5.0, where human–AI collaboration is central, judicial engagement with artificial intelligence becomes a key safeguard for fundamental rights. This article examines how India's courts can shape AI governance by learning from the United States and the European Union. Indian jurisprudence in K.S. Puttaswamy v. Union of India, Anuradha Bhasin v. Union of India, Shreya Singhal v. Union of India, and Selvi v. State of Karnataka balances innovation with rights, yet direct engagement with AI disputes remains limited. The US judiciary confronted these concerns in State v. Loomis and Houston Federation of Teachers v. Houston ISD, raising due process, fairness, and transparency questions without consistent federal guidance, while the EU adopted a rights-based approach through Schrems I and Schrems II and the recent AI Act. Given caste bias, the digital divide, and weak enforcement capacity, India should blend constitutional values under Articles 14, 19, and 21 with comparative doctrines to evolve a hybrid model safeguarding rights and responsible AI innovation.

Keywords: AI; Human; Judiciary; Jurisprudence; Technology.

1. Introduction

Nations all over the world are moving towards the dawn of the fifth industrial revolution, known as Industry 5.0. It is the new next phase of industrialisation after Industry 4.0, which sees humans working alongside advanced technology and A.I.-powered robots to enhance workplace processes (TWI Ltd, 2025). Rather than highly intelligent machines replacing human beings from the workplace altogether, Industry 5.0 emphasises the collaboration between both (Breque et al., 2021). Basically, artificial intelligence, robotics, and sensor networks work alongside human creativity, judgment and value-driven decision-making (Xu et al., 2021).

India, with national initiatives such as Skill India and SAMARTH Udyog Bharat 4.0, is preparing itself for the highly anticipated era of Industry 5.0 (Amity Institute of Training & Development, 2025). PwC research finds that 93% of Indian manufacturers are already embracing Industry 5.0 to drive both sustainable practices and boost revenues (PwC India, 2024). Further transition can be seen in the automotive industries, like that of Bajaj Auto (Universal Robots A/S, 2025), where robots assist in assembling components with precision. Similar patterns can also be observed in a variety of industries in India, like the Textiles and Packaging industry or CNC factories. That is why Industry 5.0 needs a broad-based governance structure now, because Industry 5.0 is not simply the next industrial revolution, but rather a new human-machine collaboration in the workplace that will push the limits of legal, ethical and institutional frameworks, and compel states to re-examine issues of accountability, privacy and fundamental rights in a world driven by AI.

The importance of such governance is evident from real-life instances where AI systems, that were intended to assist humans, have failed to do so, leading to serious consequences (O'Neil, 2016). For example, an Uber self-driving car hit and killed a passerby in Tempe, Arizona. Investigations revealed that segment two of the artificial intelligence system failed to recognise the pedestrian as a human being, thus resulting in the fatal incident (Marshall, 2025). Another instance would be when the UK's Metropolitan Police trialled their facial recognition system, and it showed that four out of five people identified by the Metropolitan Police's facial recognition technology as possible suspects are innocent (Manthorpe & Martin, 2019). These are just a few of many examples that demonstrate why the partnership of humans and AI requires legal

norms to ensure that human dignity, autonomy and consent are preserved in environments where AI assists, monitors or evaluates people (Mittelstadt et al., 2016).

Now, despite the fact that India is already in the early stages of transitioning to Industry 5.0 and the need for governing the changes it will bring along is becoming increasingly urgent and detrimental if left unchecked, India still lacks a comprehensive legislative framework to regulate AI technologies. And while the government is in the process of drafting a framework to regulate AI technologies as can be observed from the Ministry of Electronics and Information Technology that analyzed existing legal frameworks and proposed recommendations to develop a comprehensive approach to ensure "trustworthiness" and "accountability" of AI systems in India (Rautray, 2025) primarily aimed at industries and workplaces, there is still no binding Act of Parliament to govern AI related issues leaving behind a dangerous policy vacuum.

This is where the role of the judiciary emerges as the first institutional responder to address ethical, legal and constitutional questions arising with the use of AI because the Courts have historically interpreted existing laws and constitutional principles in order to fill policy gaps. During the Industry 4.0 era, there was a mass collection and processing of personal data providing a unified digital identity system and data-driven services. Yet, at that time, there were no comprehensive data privacy laws to govern the same. Then came the case of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) (Justice K.S. Puttaswamy v. Union of India, 2017), where the Court held that Article 21 of the Constitution included the Right to Privacy, which later laid down a legal foundation for data privacy in India and the new Digital Personal Data Protection (DPDP) Act are all legislative responses to this judiciary's first strike. This showcases how the judiciary, by filling the gap that was created as a response to technological shift and by establishing a guiding principle that aligns with the Constitutional values, has led to subsequent legislative action.

Now, as India steps into Industry 5.0, where algorithmic decision-making and workplace automation will redefine the traditional structure of workplaces in unpredictable ways and at a breakneck speed, the nation still lacks a policy. Hence, the role of the judiciary is more crucial. Because its decisions serve two purposes. They solve immediate constitutional dilemmas. And they lay the foundation for a comprehensive legislative framework that will provide clear boundaries within which future governments can operate with confidence.

Thus, the article has a comprehensive look at how the Indian judiciary has confronted, responded to and sought solutions for both legal and ethical issues raised by AI technologies. Besides, it draws a cutting-edge comparative light through the judiciaries of the United States and the European Union on these matters. Overall, this article intends to identify some general judicial principles as well as primary judicial rules, and to provide an ahead-of-its-time framework for reading future case-law that will not only guide this Indian judiciary in its own approach but also guide Indian laws to govern the Industry 5.0 revolution in an effective and increasingly rights-protecting one that lasts.

2. Rationale for Comparative Study

The judiciary has played an important role in resolving disputes that arise from technological evolution. A number of basic principles on privacy vis-à-vis digital development have been confirmed by the judiciary in India. It suggests the court sets limits to what will work better for everyone, and can help fill policy gaps when those policies are not working. This judicial role, embodied by the Indian judiciary, is not unique. Courts throughout the world have a duty to interpret laws consistently in order to cope with what is presented by rapid technological progress.

Thus, this article's comparative analysis is done with two key jurisdictions the United States and the European Union both of which have been the forerunners in technological advancements and, more importantly, have witnessed landmark judicial interventions in shaping technology-related rights. For instance, in Carpenter v. United States (2018) (Carpenter v. United States, 2018), the US Supreme Court had to assess whether the Third-Party Doctrine, a 1970s legal idea — which states that information shared by choice to a third party loses privacy rights — could be applied to digital data recorded in phones, so that they can be accessed without a warrant. Despite the absence of specific legislation addressing smartphone data, the Court stepped in to extend the constitutional principles of privacy and liberty to rule out the Third-Party Doctrine as non-applicable to modern cell phone data, affirming that search warrants are mandatory in order to access such data. This judgment effectively set a new constitutional baseline that the US legislators must now consider before drafting laws on digital privacy and government surveillance. Similarly, the Court of Justice of the European Union also serves as a great example in the case of Google Spain SL v. AEPD (2014) (Google Spain SL v. AEPD, 2014), wherein the judiciary interpreted existing data laws to create a new digital right. The CJEU established the "right to be forgotten" under the EU Data Protection Directive, which gave individuals the right to request search results that had their personal information removed, especially if the information is outdated, unnecessary and excessive. This later became a foundational principle that was codified directly into Article 17 of the EU's General Data

Protection Regulation (GDPR) (European Parliament & Council, 2016), perfectly illustrating the transition from judicial intervention to comprehensive legislation.

While these cases dealt with the issues of Industry 4.0, focusing on data and digital technology rather than AI, they do lay down foundational principles that can govern future technological advancements and mainly illustrate the judicial pattern where courts step in the absence of comprehensive legislation to regulate technological disputes and later provide blueprints for future legislation. The same pattern of development is now being repeated in the current Industry 5.0 era, especially in the courts of the United States and the European Union, which have already started grappling with the difficult problems of algorithmic bias, autonomous systems and AI accountability, and the legal principles that emerge from their judgments therefore provide a convenient basis for comparative analysis.

These judiciaries also serve to be ideal comparative materials as all three jurisdictions share similar constitutional democracies like India which has its Fundamental Rights, the US has a written constitution with a 'Bill of Rights' and the EU's legal order has the 'Charter of Fundamental Rights of the European Union' which is legally binding on EU institutions and member states while implementing EU law that place significant power on an independent judiciary to protect citizen's rights. They all share a similar power where the judiciary plays a central role in reviewing state action. In India, the Supreme Court is empowered under Articles 32 and 226 to strike down laws or executive action inconsistent with fundamental rights. The United States Supreme Court, since Marbury v. Madison (1803) (Marbury v. Madison, 1803), has developed robust doctrines of judicial review. Similarly, the Court of Justice of the European Union (CJEU) ensures that EU institutions and member states comply with the EU treaties and the Charter of Fundamental Rights. The fact that the legislature may often be slow in responding to technological development makes the strength of judicial review key to the role of the judiciary in policymaking and protection of rights.

This comparative study of technology and private law is also of relevance to India, where it can be used to respond to challenges that have not yet arisen, because the comparison is intentional and prospective, and it seeks to identify early principles that will inform legal and regulatory thinking going forward. In this article we consider the principles developed by the judiciaries of the United States and the European Union, specifically transparency, accountability and human oversight, to help develop a reasoned framework for regulating the future development of AI. Ultimately, this comparative study seeks to support judicial responses and policy-making in a manner that is academically grounded, internationally informed, and attentive to the challenges of Industry 5.0.

3. Judicial Engagement with Technology in India

In many ways, the Indian judiciary has been a front-runner in technology, and is arguably one of the more technologically advanced judicial systems in Asia, but the legislative implications of these changes have however been relatively unexplored and underdeveloped. Prior to comparing the approaches taken by the courts in the US and the EU, it would be helpful to understand the extent to which Indian courts have advanced technologically, and where they are today in assisting lawmakers in responding to legal challenges created by new technologies such as AI. Although the Indian courts have not yet delivered a judgement that is directly targeted at the broader regulation of AI systems in the workplace, or human-machine collaboration, they have created a constitutional framework for the adjudication of technology-related issues through a rights-based approach, and through a series of path-breaking judgments, the courts have developed a robust jurisprudence on privacy, proportionality, freedom of expression and protection against technology misuse, which are a useful starting point for future legislation in the area of AI governance (Arun, 2019).

Indian judiciary's journey with technology began way back in the pre-digital age with the case of Selvi v. State of Karnataka (2010) (Selvi v. State of Karnataka, 2010), which still continues to shape the boundaries of lawful technological intervention. In this case, the Court dealt with unique technological methods used to extract information from an accused, such as narco-analysis, polygraph tests, and brain-mapping. The question of how far the State can use technology to override individual consent was answered in this case where the Court basically held that State cannot use any technology to forcibly invade a person's mind, private thoughts, memories or choice as it would violate Article 20(3) which provides protection against self-incrimination and Article 21 which guarantees right to life and personal liberty. This judgement is significant as it acts as a shield against any future technology that attempts to do the same thing and provides the limits that need to be taken into account for any future laws, especially those confronting Industry 5.0 tools like AI-driven emotion tracking or workplace neuro-technology, ensuring that an individual's cognitive liberty is not violated.

Then comes the case of Shreya Singhal v. Union of India (2015) (Shreya Singhal v. Union of India, 2015), which drew a constitutional boundary as to how the government can regulate digital technology. This case

came to be after two young women were charged under Section 66A of the Information Technology Act, 2000 (Parliament of India, 2000), which criminalised sending 'offensive' or 'annoying' messages online. The judgement struck down Section 66A as unconstitutional, stating that freedom of speech and expression guaranteed under Article 19(1)(a) applies equally to digital spaces too, and that laws regulating online activity must not be vague or overbroad and must meet the standards provided under Article 19 (2). This case is not just isolated to re-affirming freedom of speech in the online and digital domain; it set rules that any attempt to regulate technology must be compatible with the Fundamental Rights and must not be vague.

In 2017, the Supreme Court established the right to privacy as a part of Article 21 in the case of Justice K.S. Puttaswamy v. Union of India (2017) (Justice K.S. Puttaswamy v. Union of India, 2017) and introduced concepts like informational privacy, data consent and purpose limitation. This judgment also introduced the proportionality test through which the judiciary can test and see if a technology or the law governing a technology that impacts privacy is constitutional. This test was put to practice in Justice K.S. Puttaswamy (Retd.) v. Union of India (2018) (Justice K.S. Puttaswamy v. Union of India, 2019), also known as the Puttaswamy II case, where the Court struck down parts of the Aadhar Act (2016) that went beyond the permissible technological limits and violated the fundamental right of privacy laid down in the Puttaswamy I judgement. Thus, this proportionality test has the potential to serve as the main tool to challenge AI-powered monitoring or algorithmic decision making. This case also sets a precedent that while the state can use technology for welfare, it must not cross certain boundaries that violate the privacy of its citizens without a legitimate and proportional basis.

The constitutional principles of privacy, free expression, and proportionality that were collectively laid down in the earlier stated landmark cases were tested in the case of Anuradha Bhasin v. Union of India (2020) (Anuradha Bhasin v. Union of India, 2020) where the Court had to find a balance between national security concerns and constitutional values of liberty and expression. It affirmed the importance of the internet in exercising fundamental rights in this modern era of ever-changing technology and linked access to the internet directly to freedom of speech and trade in this digital era. Applying the proportionality test, the Court also emphasised that any restrictions on accessing the internet must be necessary, least restrictive, proportionate and time-bound. In addition, the Courts recognise that as the exercise of rights has entered an age increasingly dependent on digital infrastructure, this is a sign that future legislation cannot concern itself alone with freeing citizens from technology; it must also be able to protect citizens' rights as accessed through technology. The way of judgments, all available as evidence, shows that the judiciary clearly addresses such technology-driven issues; parliament can now take for granted a set of constitutional principles that it later on codifies according to what its future legislative work calls for in governing newer technological advances. Indian courts have also established that constitutional provisions cannot be static and have to be interpreted in a dynamic manner to safeguard individual rights from the evolving technology (Bhatia, 2019).

This interpretive adaptability seen in these case judgments has the potential to serve as a constitutional compass not just for the judiciary in addressing the unprecedented questions that are bound to be asked with Industry 5.0's fusion with human intelligence and artificial intelligence, but also for the legislators as they begin to frame laws for Industry 5.0. And this is especially relevant considering the fact that India is currently entering the new phase of technological disputes where the boundaries of these constitutional principles are being pushed, as can be observed in the ongoing case of Asian News International (ANI) v. OpenAI brought before the HC of Delhi. This case revolves around ANI's allegations that OpenAI used its news content to train ChatGPT without permission and that ChatGPT falsely attributed fabricated news stories to the agency, damaging its reputation and potentially spreading misinformation (Panwar, 2025). Though the focus of this case is more on copyright and misinformation, it reflects the broader tensions that will define Industry 5.0 by highlighting the questions of authorship, accountability and ethical AI use. Cases like ANI v. OpenAI offer an early glimpse into the kind of legal and constitutional challenges that Industry 5.0 will intensify, which is why it becomes imperative to look at the judicial responses of the United States and the European Union that can inform and refine both India's evolving judicial approach to technology and its future legislative framework.

4. Comparative Judicial Approaches

4.1 United States

Like India, the US also does not have a federal law on AI, and as a consequence, its courts have been dealing with AI-related challenges through constitutional values. The analysis of these judgments provides us with, not a model that needs to be copied, but rather a source for newer constitutional principles. They provide us with a framework built on algorithmic due process and transparency, thereby offering powerful guidance

to the Indian judiciary in shaping its own constitutional response to AI and, by extension, providing a clear set of principles for the Indian legislators to codify into a national AI governance framework.

In the industrial era, where human creativity and judgement work side by side with the analytical power of AI, a fundamental legal challenge arises (Calo, 2015). What happens when the human worker's AI partner, which might be assisting in critical decisions or evaluating their performance, operates as a 'black box? The black box dilemma can basically be defined as our inability to fully understand an AI's decision-making process and predict its outputs or decisions. (Singh & Rafiq, 2025) This opacity in these systems, where the AI's reasoning is a secret and is unexplainable, makes it impossible for humans to challenge it, making it a direct threat to the basic principles of fairness, which are enshrined in most justice systems (Pasquale, 2015). This very issue was confronted by the US judiciary, revealing their commitment to upholding due process by demanding transparency and thus establishing rules for this new human-machine relationship.

In the case of State v. Loomis (2016) (State of Wisconsin v. Loomis, 2016), the SC of Wisconsin examined whether a sentencing judge could rely on a risk assessment algorithm known as COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), whose internal functioning was a secret and was inaccessible to both the accused and the judge. Eric Loomis, who was flagged for being at high risk of re-offending by this algorithm and was sentenced to six years in prison on this basis, argued that using such a 'black box' system violated his right to due process as he could neither challenge or understand the reasoning behind the algorithm in labelling him as a high-risk offender. While the judgment did permit the use of COMPAS, it clearly drew a strong procedural safeguard line by stating that it could only serve as a supplementary aid in sentencing and cannot be used as a determinative factor in deciding punishment. The judgment also contended that COMPAS must carry explicit warnings acknowledging the system's group-based nature, possible bias and inability to provide individualised and case-specific assessments.

Then the concern over fairness and transparency in AI-assisted decision making emerged in the workplace and in the administrative context, where the US judiciary had to establish its stance once again in the case of Houston Federation of Teachers v. Houston Independent School District (2017) (Houston Federation of Teachers v. Houston ISD, 2017). Houston Independent School District (HISD) adopted a proprietary algorithm called EVAAS, whose inner workings were inaccessible to both the employees and school administration, which generated 'effectiveness scores' that were used to evaluate and terminate teachers. The federal court held that such opacity violated the teacher's right to procedural due process since they were denied the right to challenge and understand the evidence used against them, and reinforced that while institutions can rely on algorithmic systems for high-stakes decision-making, they must ensure fairness and explain how these systems work (Barocas & Selbst, 2016).

The US Court's articulation on the principle of algorithmic transparency and insistence on due process deeply resonates with Article 14 and Article 21 of the Indian Constitution and can be meaningfully adopted by India, considering the fact that since the Maneka Gandhi v. Union of India (1978) (Maneka Gandhi v. Union of India, 1978), the Indian Courts have stressed on processes being fair, just and non-arbitrary, which is a standard rooted in transparency and accountability (Citron & Pasquale, 2014). Furthermore, the core values laid down in the 'Loomis Warning', which cautions the judges about the limitations and biases of algorithmic tools, have the potential to serve as a model for lawmakers on what procedural fairness can look like in the age of AI. For India, this is also a guide to a future AI law that mandates transparency in high-stakes areas—meaning human decision makers must legally understand the limitations of tools they use made by machines.

The decision in Houston Federation of Teachers v. Houston Independent School District, since it was handed down by a federal court, carries much more weight than State v. Loomis. What makes this distinction so significant is that it serves to illustrate a certain genuine dissatisfaction with the US Judiciary, one that is probably not unfounded. This is uneven judicial supervision, wherein similar issues can be decided differently according to the state in which they occur. It exposes a need for consistency if pertinent reasoning and outcomes one way or another (ie, implying how people will live) are to guide the nation. This exposes a need for consistency in the judicial reasoning and decisions that can guide the nation until there is comprehensive legislation. Though the Indian Judiciary operates in a unitary constitutional framework, this observation places importance on the need for a uniform procedural safeguard for better clarity.

Another, less obvious, but equally important, principle that emerges from these two cases is the principle of accountability, though neither State v. Loomis nor Houston Federation of Teachers v. HISD framed the issue in terms of where accountability should lie for AI-assisted decision-making, both cases implicitly hold human and institutional actors accountable rather than allowing AI systems to be used as a legal shield. In Loomis, the Wisconsin Supreme Court recognised the limitations of the COMPAS tool and explicitly stated that judges would remain accountable for sentencing decisions, while in the Houston case, the federal court signalled that the school district could not pass the buck to the EVAAS algorithm and that administrators remained accountable for protecting fairness and ensuring the accuracy of outcomes

generated through AI-assisted systems. This principle of accountability is especially important for Indian lawmakers, because it reminds them that humans and institutions cannot abdicate responsibility simply because an AI system is involved (Selbst et al., 2019). Consequently, the US judiciary has shown how constitutional interpretation can be developed to respond to the challenges of AI-driven decision-making.

Through the principles of due process, transparency, and accountability, American courts have established a preliminary benchmark for fair AI governance, and India can draw on these reference points since they demonstrate the significance of procedural safeguards, institutional responsibility, and judicial oversight. As India evolves its own AI governance framework, these lessons serve as a warning, as well as a guide, to prevent the diminution of justice, equality, and liberty in the age of artificial intelligence, therefore, they are crucial for India's development of a fair and just AI governance framework.

4.2 European Union

Unlike India and the United States, the European Union has already enacted a legal framework for the governance of artificial intelligence, namely the Artificial Intelligence Act, which regulates the development, deployment and use of AI systems in the European Union (Lynskey, 2015). It is based on a risk-based approach, i.e., AI systems are classified on the basis of the level of risk they pose, and obligations and restrictions imposed on them depend on this classification, therefore it puts a strong emphasis on transparency, explainability, human oversight and accountability in order to ensure that AI systems do not operate outside meaningful human control (Wachter et al., 2017). The EU AI Act did not emerge in a legal vacuum, but is part of a legal culture deeply rooted in landmark judicial decisions and, in particular, the General Data Protection Regulation, which, adopted in 2018, grants individuals important rights over their personal data and establishes important principles such as data quality, transparency, accountability and human control over automated processing (Kuner, 2007). These principles have had a profound impact on the structure and philosophy of the EU AI Act, while the GDPR, however, did not evolve in a vacuum either, but was developed through a long history of judicial interpretation of privacy, dignity and data protection within the European Union. Some of these cases have established crucial principles that now extend to the EU AI Act, and these cases serve to be valuable for this comparative analysis as they can guide India in both the judicial reasonings and legislative actions towards crafting a rights-based framework for AI governance.

In Schrems v. Data Protection Commissioner (2015) (Schrems v. Data Protection Commissioner, 2015), the court found that US surveillance laws allowed disproportionate access to EU citizens' data without judicial redress, which violated EU Charter of Fundamental Rights, notably Article 7, which deals with privacy and Article 8, which deals with data protection and thus invalidated the EU-US Safe Harbour framework, which allowed this transfer of EU citizens' personal data to the US. This case established that EU citizens' data rights are continuously being protected under EU standards, even though they are transferred abroad, and this principle of extraterritorial rights protection is the backbone of the EU AI Act, as can be seen in Article 2 (European Parliament & Council, 2024a) of the Act, ensuring that the AI Act applies to all AI systems entering the EU market, even if it is developed outside. India can learn from this borderless approach, which would respect Indian citizens' data and rights when it is handled by a foreign AI system, creating a globally accountable AI framework (Bygrave, 2014).

The EU-US Privacy Shield, which was a replacement for Safe Harbour, was challenged, arguing that the US surveillance laws continued to provide insufficient protection for the personal data of EU citizens, in the case of Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems (2020) (Data Protection Commissioner v. Facebook Ireland & Schrems, 2020). The courts observed that US surveillance programs still did not provide effective judicial remedies and invalidated the Privacy Shield. It also held that companies are responsible to verify, case by case, that foreign laws do not prevent the protection of EU rights, making sure that data protection compliance is substantive and continuous and reaffirmed extraterritorial accountability. This principle was extended to the EU AI Act as it mandated that AI developers must ensure training datasets are lawfully and ethically sourced as observed in Article 10 (European Parliament & Council, 2024b) clubbed with Article 16 (European Parliament & Council, 2024c) which makes AI developers accountable. India can mirror this accountability structure and embed these principles in its policy making to help prevent the misuse of citizen data and build a trustworthy AI system that aligns with fundamental rights.

The case of Digital Rights Ireland v Minister for Communications (2014) (Digital Rights Ireland v. Minister for Communications, 2014), offers a new angle on the relationship between technological surveillance and constitutional rights. The Court of Justice of the European Union struck down the EU's Data Retention Directive, which required telecommunication companies to store citizens' data for up to two years for law enforcement purposes, finding such mass and indiscriminate collection of data violated rights to privacy and data protection under the EU Charter of Fundamental Rights. This case introduced the principle of necessity and proportionality, stating that any interference with privacy must be necessary and limited to specific, justified purposes. And this principle was carried forward to the AI Act to govern the

datasets and decision-making processes of AI systems, with Article 10 (European Parliament & Council, 2024b) of the Act stating that data used to train high-risk AI systems must be "relevant, representative, free of errors, and complete". This basically meant that only necessary data can be appropriately used in order to ensure fairness and accuracy. Additionally, the Act also regulates developers to assess whether the impact of a high-risk AI system used by public authorities on citizens' rights is necessary and proportional to its intended goal. For India, which already has its own proportionality test introduced in Justice K.S. Puttaswamy v. Union of India (2017), the codification of such principles in the AI Act provides a legislative model that the lawmakers can adopt for operationalising the judicial doctrines of privacy and proportionality within the emerging AI realm (Kaminski, 2019).

Considering all these developments and judicial-legislative continuity within the EU's governance model, it can be argued that the EU represents an advanced stage of rights-based AI governance, where judicial interpretation has directly evolved into legislative codification. Through some of the many landmark cases mentioned here, such as Schrems I & II, Digital Rights Ireland, it can be observed that the EU courts have built a constitutional ecosystem that has translated into the EU AI Act. The Act gives effect to these judicial doctrines in a real-life manner, ensuring both that AI systems operate from a fundamentally human-centred base and that they remain fundamentally just too. Three lessons from the European Union experience are particularly relevant for India's regulatory project, and the first is that constitutional rights must be integrated at the very centre of the AI regulatory framework rather than being treated as an external safety valve or an afterthought. The second is that meaningful transparency must be guaranteed in high-stakes AI systems, particularly in contexts where such systems impact rights, opportunities or access to essential services, and the third is that accountability mechanisms must be established not just for domestic actors but also for foreign AI suppliers operating in or servicing the Indian market. In this sense, the EU experience gives India a more effective model for the translation of broad constitutional principles into a coherent statutory framework, one that promotes innovation without sacrificing fundamental rights at the altar.

5. Challenges and Implementation of Adapting Foreign Models to India

The US and EU make good case studies for a moral and rights-based framework for AI governance, but transplanting such models in India would not be straightforward because the socio-legal and infrastructural conditions in India are quite different from those in Western jurisdictions. Transplanting foreign regulatory structures without any localisation can lead to conceptually sound but practically unworkable legislation, therefore, these challenges need to be taken into account before designing an AI governance model that is not only technologically sound, but also within the constitutional framework, institutional capacity and social realities of India.

One of the most fundamental challenges that needs to be considered is India's tech and infrastructure gap. While India is marching towards Industry 5.0 and AI-enabled workplaces, an underlying reality still exists in the nation, starting with limited digital literacy. A report made by Oxfam in 2022 reported that only 38% of households in India are considered digitally literate (Mahendru et al., 2022). Despite the increase in digital access over the recent years, NSSO (National Sample Survey Office) data reveals a staggering disparity: only 24% of rural households have internet access, compared to 66% in cities (NIIT Foundation, 2024) which showcases the continuing existence of digital divide in India. Now, the AI governance principles of transparency and accountability established by the United States and the European Union courts are built on certain assumptions of a digitally literate populace. From an Indian standpoint, importing such foreign frameworks into the workplace, especially in small towns, rural factories, informal sector units, without modifications, would be extremely problematic. For instance, if a factory in a tier-2 town employing workers with low digital literacy introduces an AI-based performance evaluation tool, but the workers do not know how to read or contest algorithmic outputs, and if the supervisors are not trained to identify biases or technical limitations in such systems, the tool would continue to function as a black box, despite formal legal requirements of transparency and human oversight. Therefore, AI governance regulations in India should not end at abstract principles but include explanation mechanisms that can be understood by those with low digital literacy, perhaps through community intermediaries, simple interfaces and regional language support.

While one of the rationales for selecting the judiciaries of the US and the EU for comparative analysis with India is because of their structurally similar constitutional systems, namely shared democratic values and powerful independence of the judiciary, India can still face constitutional challenges in applying the findings of the US and the EU. Issues can arise because alignment in principle does not automatically mean to compatibility in practice. Therefore, any principles taken from foreign judiciary must survive the test of India's golden triangle. The Golden triangle comprises Articles 14, 19 and 21 together, ensuring equality, freedom and the right to life and personal liberty, which ultimately creates a rights-based framework.

The principle of due process as it exists under Article 21 is more substantive than the one present in the US. An AI system that meets the procedural standards of fairness in the US might still fail in India if its decisions lead to an outcome that offends human dignity or is disproportionate. Thus, while deriving principles for AI governance from the US judiciary, the impact of the algorithmic decision must align with fairness and reasonableness, not merely in design. Similarly, the guarantee of equality under Article 14 goes beyond formal equality. Any state or quasi-state action that lacks a rational basis and is arbitrary is unconstitutional. Hence, the tolerance shown in the State v. Loomis case, where algorithmic opacity was tolerated with caution, is unlikely to happen in India, given its strict stance against arbitrariness. So, while the lesson from these cases is helpful and can surely guide in India's development of AI governance law, they must be interpreted through the lens of India's own constitutional doctrines of non-arbitrariness. Lastly, Article 19(1)(g), which protects the freedom to practice any profession, read along with non-arbitrariness and proportionality, is highly relevant in the context of this digital climate and must also be accounted for when integrating foreign judicial principles. Therefore, the constitutional challenge lies in ensuring that India absorbs the best global practice without diluting India's constitutional guarantees of equality, liberty and dignity and remains firmly anchored to India's 'golden triangle'. Therefore, the most crucial implementation strategy is constitutional grounding.

But apart from the infrastructural and constitutional challenges, there are deeper social and cultural inequalities that India has to consider before bringing in any Western AI governance model, because foreign AI systems are built in response to the social context they operate in, such as racial or gender biases. India's social context is far more complex, with its caste hierarchies, religious diversity, linguistic plurality, and sharp regional disparities, and this is crucial because AI systems are not inherently neutral; they are only as fair as the data they are trained on, and the social assumptions encoded in that data (Barocas et al., 2019). Training an AI model on data with bias, such as historical or representational bias, could lead to biased or skewed outputs that might unfairly represent or otherwise discriminate against certain groups or individuals (Rogers & Jonker, n.d.). For instance, Siva Mathiyazhagan, in his report to Thomson Reuters, stated that "if a chatbot is asked to name 20 Indian doctors and professors, the suggestions are generally Hindu-dominated-caste surnames." (NLIU-Cell for Law & Technology, 2025). Dalits and Muslims are often misrepresented or excluded by algorithms that classify their communities as "high risk" due to historical poverty (Raza, 2025). Gender bias enforced by AI is a global issue and manifests in particularly troubling ways in India. The algorithm for credit scoring is biased and they reject women's loan applications or give them low ranks (Dethe & Dethe, 2025). An AI Indian facial recognition tool was reported to have failed in identifying Indian women more than Indian men (Mehrotra, 2021). These examples illustrate exactly why India's AI governance framework cannot be a blind replica of Western models because the anti-bias considerations placed in the Western models, while valuable, are not enough to properly regulate the complex realities of AI discrimination in India. Instead, India's framework must be contextually grounded, explicitly addressing caste, religion, gender and regional disparities. This requires building an inclusive dataset, ensuring diversity in AI development teams and laying down systematic review or testing of an AI system to check whether it produces unfair, discriminatory, or skewed outcomes, so that technology is governed in line with India's constitutional values of equality, non-discrimination and dignity.

The principal question that India would have to answer, when importing foreign models of AI governance, is one of institutional enforcement, because even if India were to craft a broad and constitutionally coherent framework, it would require a capable institution to enforce it. The EU's AI governance model is enforced by Data Protection Authorities that have spent decades developing enforcement muscles, whereas India does not have a comprehensive legislation exclusively regulating AI, but it does have an institutional foundation that could support AI governance. Since data is the indispensable fuel that powers AI systems, the Data Protection Board, which has been set up under the Digital Personal Data Protection Act, 2023, could become a critical institution for AI oversight; however, unlike the EU's regulators, which are more mature and tested enforcement bodies, the DPB in India is a new institution with unformed precedent, untrained personnel, and inadequate technical infrastructure. This is a large gap between legislative ambition and administrative capacity, and to bridge this gap, India would need to make significant investments in building the institutional and technical capacity of the DPB, so that future AI laws have a transformative impact rather than staying symbolic.

An alternate solution could be building a brand-new, specialised body that only focuses on AI governance, making it more agile and expert-driven. But this raises a question as to how India can properly regulate technology that is constantly evolving. The new regulatory body must find a balance between innovation and regulation. This is where the concept of the sandbox regulatory framework becomes relevant, as it can help equip the enforcement bodies with empirical knowledge and contextual understanding of the AI system. Regulatory sandboxes are tools that are used by businesses to assess and explore new and innovative products, services or businesses under the supervision of a regulator for a

limited period of time and they support regulatory learning, i.e. the formulation of experimental legal regimes to guide and support businesses in their innovation activities under the supervision of a regulatory authority (Madiega, 2022). For instance, the companies developing AI systems, with the help of the sandbox mechanism, can operate in a closely monitored space, and the regulators and experts will then draw observations on how the system behaves and identify potential biases or harm. This evidence gathered from these controlled experiments can be combined with the AI governance law drafted from existing legal insights and best international practices, enabling adaptive and context-specific regulatory action by the enforcement body.

However, as India seeks to study the global judicial treatment of AI governance and frame its own AI law, it must ensure that the law is anchored in the constitutional values of the country, and India should begin with a rights-based charter, congruent with constitutional commitments, institutional readiness and social inclusiveness before introducing a full-fledged AI bill. This would ensure that governance of technology is not merely theoretical or imported but rooted in the lived experiences of people and the social and institutional realities of India.

6. Proposal for a Hybrid Framework

The judicial AI governing framework proposed in this paper seeks to blend global best practices with the unique needs posed by its constitution. In such a case, judicial standards must also be adequately restructured to maintain justice. This new hybrid judicial model, which is proposed within the framework of Articles 14, 19 and 21 of the Constitution of India as the context for its attempted adoption, adopts the EU rights-based approach (which emphasises privacy and explainability) at its core while also taking on board elements from the United States, such as focus on accountability and due process. In this way ultimately interweaves these into a single concept tied back to Indian Ideas of justice. This approach recognises that although foreign experiences are invaluable (Choudhry, 2006), transplanting solutions envisaged in distant countries' constitutions into our own set-up and social circumstances can produce workable ones with unintended consequences.

For the new field of judicial guidance and regulations surrounding artificial intelligence, this paper suggests that we should adopt a Judicial AI Principles Charter. First of all, if decisions made by AI-backed systems are to be transparent and explainable, then it follows that they should not resemble black boxes: if judges and litigants (indeed, all groups) cannot understand them at all, such an opaque manner of decision-making runs counter to procedural justice (Hildebrandt, 2015). Second, proportionality is crucial: the courts must guard against blind trust in AI, making sure instead that its social benefits indisputably outweigh any risks to rights, which coincides with a principle found in Article 21 of India's Constitution, known as the Supreme Court's proportionality test. Third, obligatory human oversight is needed to maintain essential accountability in critical matters: despite any practical convenience that AI may bring for running affairs with high stakes such as finance or security considerations, human judgment should always come first, as agreed by all parties involved. India needs to establish a liability framework which apportions responsibility for the harm caused by AI amongst the developers, deployers and the State, and this will ensure that technology is not treated as an independent legal actor or a shield to pass the buck, but is recognised as a tool whose consequences remain attributable to the human and institutional actors who design, deploy and rely on it.

The initiative brings the global movement of responsible AI in sync with India's constitutional scheme of fundamental rights and reinforces the view that there can be no technological progress without justice, equality and human dignity.

7. Conclusion

Industry 5.0 has brought India into the AI age, but a multitude of questions have to be answered as far as law, justice, infrastructure, and society are concerned, and all these questions can only be answered by a AI governance framework specifically for India. India cannot adopt the judicial AI models of the European Union and the United States, but instead has to create a hybrid model by drawing from the universal regulatory principles and, at the same time, ensuring that the same is rooted in the constitutional values of India that are enshrined in Articles 14, 19, and 21 of the Indian Constitution. This model must also ensure that AI systems remain transparent, explainable and accountable in order to ensure that procedural fairness and fundamental rights are protected, and AI must, therefore, be used with caution and moderation and only in cases where its social benefits far outweigh its risks. Human agency must similarly remain at the centre of an AI governance framework to prevent accountability from being obscured in layers of automated decision-making, and India also needs a clear liability framework to fairly distribute accountability among developers, deployers, product stakeholders and state institutions in accordance with emerging laws and regulations.

India's AI governance framework must also be sensitive to its social realities, because the country's low levels of digital literacy, caste, religious and gender-based inequalities and institutional capacity gaps cannot be ignored. This is why institutions such as the Data Protection Board must be strengthened, and flexible regulatory tools such as sandboxes must be utilised to test innovation in a responsible and controlled manner. In the face of such a revolution, India's AI regulatory framework of the future will need to walk the tightrope between technology and constitutional morality, because it must ensure that AI does not nullify human dignity, non-arbitrariness, or justice, but rather aligns citizens to a rights-respecting and inclusive technological future. Consequently, if India is to emerge as a responsible leader in the global AI revolution, its approach to AI governance must be grounded, contextual, rights-based and genuinely responsive to the needs of its people.

Acknowledgement
None
Data availability statements
Data sharing not applicable to this article as no datasets were generated or analysed during the current study.
Funding
This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.
Conflict of Interest
The authors declare that they have no potential conflict of interest.

References

1. Amity Institute of Training & Development. (2025). Industry 5.0 is here: Are you ready for the future?https://aitd.amity.edu/blogs-detail.php?title=industry-5-0-is-here-are-you-ready-for-the-future
2. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).
3. Arun, C. (2019). AI and the global south: Designing for other worlds. In M. D. Dubber, F. Pasquale, & S. Das (Eds.), The Oxford handbook of ethics of AI (pp. 587–606). Oxford University Press.
4. Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. California Law Review, 104(3), 671–732.
5. Barocas, S., Hardt, M., & Narayanan, A. (2019). Fairness and machine learning: Limitations and opportunities. fairmlbook.org.
6. Bhatia, G. (2019). The transformative constitution: A radical biography in nine acts. HarperCollins India.
7. Breque, M., De Nul, L., & Petridis, A. (2021). Industry 5.0: Towards a sustainable, human-centric and resilient European industry. Publications Office of the European Union.
8. Bygrave, L. A. (2014). Data privacy law: An international perspective. Oxford University Press.
9. Calo, R. (2015). Robotics and the lessons of cyberlaw. California Law Review, 103(3), 513–563.
10. Carpenter v. United States, 585 U.S. 394 (2018).
11. Choudhry, S. (Ed.). (2006). The migration of constitutional ideas. Cambridge University Press.
12. Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. Washington Law Review, 89(1), 1–33.
13. Data Protection Commissioner v. Facebook Ireland Ltd. & Maximillian Schrems, Case C-311/18, ECLI:EU:C:2020:559 (CJEU July 16, 2020).
14. Dethe, A., & Dethe, S. S. (2025). Credit gap: Do algorithms deny loans to women borrowers? Explains CEO of Women's World Banking. ETBFSI. https://bfsi.economictimes.indiatimes.com/news/banking/credit-gap-do-algorithms-deny-loans-to-women-borrowers-explains-ceo-of-women-world-banking/118517653
15. Digital Rights Ireland Ltd. v. Minister for Communications, Joined Cases C-293/12 & C-594/12, ECLI:EU:C:2014:238 (CJEU Apr. 8, 2014).
16. European Parliament & Council. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation), Article 17. Official Journal of the European Union.
17. European Parliament & Council. (2024a). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (AI Act), Article 2: Scope. https://artificialintelligenceact.eu/article/2/
18. European Parliament & Council. (2024b). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (AI Act), Article 10: Data and data governance. https://artificialintelligenceact.eu/article/10/

19. European Parliament & Council. (2024c). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (AI Act), Article 16: Obligations of providers of high-risk AI systems. https://artificialintelligenceact.eu/article/16/
20. Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Case C-131/12, ECLI:EU:C:2014:317 (CJEU May 13, 2014).
21. Hildebrandt, M. (2015). Smart technologies and the end(s) of law: Novel entanglements of law and technology. Edward Elgar Publishing.
22. Houston Federation of Teachers v. Houston Independent School District, 251 F. Supp. 3d 1168 (S.D. Tex. 2017).
23. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
24. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1 (India).
25. Kaminski, M. E. (2019). The right to explanation, explained. Berkeley Technology Law Journal, 34(1), 189–218.
26. Kuner, C. (2007). European data protection law: Corporate compliance and regulation (2nd ed.). Oxford University Press.
27. Lynskey, O. (2015). The foundations of EU data protection law. Oxford University Press.
28. Madiega, T. (2022). Artificial intelligence act and regulatory sandboxes. European Parliamentary Research Service.
29. Mahendru, A., et al. (2022). India inequality report 2022: Digital divide. Oxfam India.
30. Maneka Gandhi v. Union of India, AIR 1978 SC 597 (India).
31. Manthorpe, R., & Martin, A. J. (2019). 81% of 'suspects' flagged by Met's police facial-recognition technology innocent, independent report says. Sky News. https://news.sky.com/story/met-polices-facial-recognition-tech-has-81-error-rate-independent-report-says-11755941
32. Marbury v. Madison, 5 U.S. (1 Cranch) 137 (1803).
33. Marshall, D. (2025). AI testing gone wrong: Lessons from real-world model failures. VMblog. https://vmblog.com/archive/2025/07/28/ai-testing-gone-wrong-lessons-from-real-world-model-failures.aspx
34. Mehrotra, K. (2021). Facial recognition technology isn't wholly accurate at reading Indian faces, find researchers. Scroll.in. https://scroll.in/magazine/1001836/facial-recognition-technology-isnt-wholly-accurate-at-reading-indian-faces-find-researchers
35. Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 1–21.
36. NIIT Foundation. (2024). Bridging the digital divide: Empowering rural India. https://niitfoundation.org/bridging-the-digital-divide-empowering-rural-india/
37. NLIU-Cell for Law & Technology. (2025). Introduction – dominated caste surnames. https://clt.nliu.ac.in/?p=1144
38. O'Neil, C. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. Crown.
39. Panwar, A. (2025). Generative AI and copyright issues globally: ANI Media v. OpenAI. Tech Policy Press. https://techpolicy.press/generative-ai-and-copyright-issues-globally-ani-media-v-openai/
40. Parliament of India. (2000). Information Technology Act, No. 21 of 2000, § 66A. Acts of Parliament (India).
41. Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.
42. PwC India. (2024). 93% of Indian manufacturers target sustainability with 2–3× profitable growth through Industry 5.0: PwC India research. https://www.pwc.in/press-releases/2024/93-indian-manufacturers-target-sustainability-2-3x-profitable-growth-industry-5.0-pwc-india-research.html
43. Rautray, R. (2025). AI governance guidelines: A glimpse into the proposed AI regulation in India. Anagram Partners. https://anagrampartners.in/archives/insights/ai-governance-guidelines-a-glimpse-into-the-proposed-ai-regulation-in-india
44. Raza, A. (2025). Rewind: Silent erasure of Dalit voices, this time by AI!. Telangana Today. https://telanganatoday.com/rewind-silent-erasure-of-dalit-voices-this-time-by-ai
45. Rogers, J., & Jonker, J. A. (n.d.). What is data bias? IBM. https://www.ibm.com/think/topics/data-bias
46. Schrems v. Data Protection Commissioner, Case C-362/14, ECLI:EU:C:2015:650 (CJEU Oct. 6, 2015).
47. Selbst, A. D., Boyd, D., Friedler, S. A., Venkatasubramanian, S., & Vertesi, J. (2019). Fairness and abstraction in sociotechnical systems. In Proceedings of the Conference on Fairness, Accountability, and Transparency (pp. 59–68). Association for Computing Machinery.
48. Selvi v. State of Karnataka, (2010) 7 SCC 263 (India).
49. Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).

50. Singh, A., & Rafiq, J. (2025). Implications of black box dilemma in the Indian legal system. Journal of Legal Research and Juridical Sciences, 4(3), 1264–1296.
51. State of Wisconsin v. Loomis, 371 Wis. 2d 235 (2016).
52. TWI Ltd. (2025). What is Industry 5.0? (Top 5 things you need to know). https://www.twi-global.com/technical-knowledge/faqs/industry-5-0
53. Universal Robots A/S. (2025). South Asian case stories on cobots – Bajaj Auto implements the first cobots in India and empowers women in manufacturing. https://www.universal-robots.com/in/south-asian-casestories/
54. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. International Data Privacy Law, 7(2), 76–99.
55. Xu, X., Lu, Y., Vogel-Heuser, B., & Wang, L. (2021). Industry 4.0 and Industry 5.0—Inception, conception and perception. Journal of Manufacturing Systems, 61, 530–535.