



NAVIGATING APPROACHES TO AI GOVERNANCE: CHARTING A PATHWAY FOR INDIA

SEPTEMBER 2023 | ISSUE 035



Navigating Approaches to AI Governance: Charting a Pathway for India

September 2023



Attribution: Meghna Bal and Vivan Sharan, *Navigating Approaches to AI Governance: Charting a Pathway for India*, August 2023, Esya Centre.

Esya Centre
B-40 First Floor
Soami Nagar South,
New Delhi - 110017, India

The **Esya Centre** is a New Delhi based technology policy think tank. The Centre's mission is to generate empirical research and inform thought leadership to catalyse new policy constructs for the future. More details can be found at www.esyacentre.org

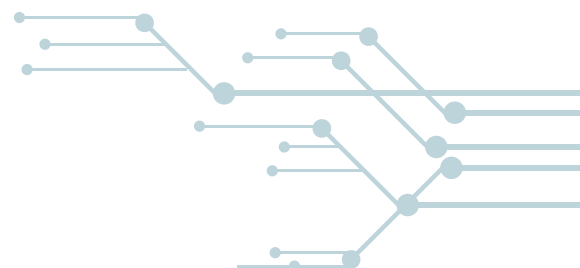
About the Authors: Meghna Bal is Head of Research at the Esya Centre, New Delhi. Vivan Sharan is a technology policy expert.

Image credit: Cover Image sourced from DALL-E - Prompt to generate the image was a Picasso oil painting of a global network of computers and artificial intelligence

© 2023 Esya Centre. All rights reserved.

CONTENTS

I. INTRODUCTION	4
II. THE AI GOVERNANCE CONTINUUM: FROM ENABLING NATIONAL STRATEGIES TO RISK-BASED FRAMEWORKS	5
1. NATIONAL STRATEGIES	5
2. GUIDELINES FOR ETHICAL AI	5
3. HORIZONTAL AI REGULATION	6
A. <i>EU ARTIFICIAL INTELLIGENCE ACT</i>	6
4. VERTICAL AI REGULATION	8
A. <i>CHINA'S DEEP SYNTHESIS PROVISIONS</i>	8
5. VOLUNTARY STANDARDS AND GUIDELINES	9
A. <i>TEC'S DRAFT STANDARD ON FAIRNESS ASSESSMENT AND RATING OF AI SYSTEMS</i>	9
6. GLOBAL REGULATION OF AI	10
III. HOW TECHNOLOGY LAWS IMPACT ARTIFICIAL INTELLIGENCE	11
A. DATA PROTECTION	11
B. INTELLECTUAL PROPERTY	11
IV. TAKEAWAYS AND CONSIDERATIONS FOR THE WAY FORWARD: BUCK THE TREND OF HORIZONTAL REGULATION	13
REFERENCES	14



I. INTRODUCTION

The clarion call for the regulation of artificial intelligence (AI) is growing louder across the world. Different jurisdictions have either introduced legislation to regulate the technology or are in the process of doing so. Aside from hard-coded laws, a bevy of voluntary standards have emerged around trust and safety concepts surrounding the deployment and development of AI.

This paper presents a roundup of different approaches to AI regulation and governance, as well as the intersection of existing legal doctrines and AI. The purpose of this paper is to put forth considerations for Indian policymakers to take into account when deciding on AI governance down the road.

II. THE AI GOVERNANCE CONTINUUM: FROM ENABLING NATIONAL STRATEGIES TO RISK-BASED FRAMEWORKS

AI governance frameworks can be divided into two buckets, enabling and risk-based.

Enabling frameworks emerged as AI's commercial potential became apparent. Now, however, as the harms of AI become apparent, nations are opting for a more risk-based approach. These include guidelines for the ethical use of AI, horizontal regulation such as the European Union's AI Act, and vertical regulation like China's deep synthesis provisions.

1. National Strategies

Broadly, these strategies target the creation of competitive advantage through the deployment of AI – either across sectors or in specific areas. Illustratively, Japan's AI strategy seeks to consolidate its progress in the field of robotics and wield AI to enhance productivity.¹ Several other nations sought to work out how AI could be co-opted to complementing the workforce (rather than supplementing it).²

2. Guidelines for Ethical AI

Guidelines for ethical AI form part of the response to trepidations about the risks presented by AI. These emanate from concerns revolving around the impact on employment, fairness and discrimination, and the use of AI by malign entities.³ A 2019 study on 84 such guidelines has found that private entities and governments account for the largest share issued and regionally these frameworks are largely concentrated in the global north.⁴ The most commonly cited principles in these frameworks are provided in Figure 1 below. The researchers note that while “no single principle appeared to be common to the whole corpus, there was emerging convergence around transparency, justice and fairness, non-maleficence, responsibility, and privacy.”⁵

Ethical principle	Number of documents	Included codes
Transparency	73/84	Transparency, explainability, explicability, understandability, interpretability, communication, disclosure, showing
Justice & fairness	68/84	Justice, fairness, consistency, inclusion, equality, equity, (non-)bias, (non-)discrimination, diversity, plurality, accessibility, reversibility, remedy, redress, challenge, access and distribution
Non-maleficence	60/84	Non-maleficence, security, safety, harm, protection, precaution, prevention, integrity (bodily or mental), non-subversion
Responsibility	60/84	Responsibility, accountability, liability, acting with integrity

Privacy	47/84	Privacy, personal or private information
Beneficence	41/84	Benefits, beneficence, well-being, peace, social good, common good
Freedom & autonomy	34/84	Freedom, autonomy, consent, choice, self-determination, liberty, empowerment
Trust	28/84	Trust
Sustainability	14/84	Sustainability, environment (nature), energy, resources (energy)
Dignity	13/84	Dignity
Solidarity	6/84	Solidarity, social security, cohesion

Figure 1: Ethical Principles Identified in 84 AI Guidelines in 2019

Source: [Jobin et. al](#)

3. Horizontal AI Regulation

Horizontal AI regulation regulates use cases of AI in accordance with the potential for societal or personal harm. It is typically agnostic of AI typologies, applying uniform set of rules to different AI systems to address concerns around safety, security, and fundamental rights.⁶ Examples of horizontal AI laws include the European Union’s AI Act, the US’ draft Algorithmic Accountability Bill, and South Korea’s Bill for Promoting and Laying the Foundation of Trust in the AI Industry. In addition, in July 2023, the Telecom Regulatory Authority of India issued Recommendations on Leveraging Artificial Intelligence and Big Data in the Telecommunications Sector where it espoused the introduction of a horizontal regulatory framework for AI.

Horizontal AI regulation largely comprises attempts to translate ethical AI guidelines into legislation. The approach is critiqued because ethical AI guidelines are generic principle-based prescriptions that are often inspired “a few high-profile cases” of harm and “based on thought experiments”, as opposed to being guided by empirical evidence.⁷ A further critique is that ethical AI guidelines treat AI like a monolith and do not distinguish between different AI models. For instance, the principle of safety is a predominantly relevant principle for “intelligent agents” or robots but not so much for discriminative AI. However, ethical AI principles make no such distinction. Consequently, the horizontal AI regulation inspired these principles largely fails to do so as well, and thus, concomitantly fails to address the specific harms emanating from different AI models.⁸ The result is a framework that impedes innovation without necessarily mitigating risks.⁹

a. EU Artificial Intelligence Act

The EU AI Act encourages the adoption of “human-centric” AI while attempting to ensure a high degree of protection from any “harmful effects” of the technology.¹⁰ It introduces rules for different categories of AI systems based on risk-profile. The first are AI systems which present an unacceptable level of risk for human safety and rights, and are therefore, banned.¹¹ These include:¹²

- a. Manipulative AI systems that either deploy subliminal techniques beyond a person’s consciousness or exploit vulnerabilities in certain categories of people to motivate them to cause harm.

- b. Social scoring systems used by public authorities to evaluate the trustworthiness of individuals based on behaviour or known or predicted traits and characteristics that may result in unfair or discriminatory treatment.
- c. The use of real-time biometric systems by law enforcement in publicly accessible spaces.¹³

The second category of regulated AI systems under the AI Act are those that pose a high risk to “health, safety, and fundamental rights”. These include:¹⁴

- a. The use of AI in “products or safety components covered by EU health and safety laws”; or
- b. “standalone” systems used in eight specified areas namely “biometrics, critical infrastructure, education and vocational training, employment, access to essential services, law enforcement, immigration and asylum management, judicial function”.

Developers of high-risk AI systems must maintain a risk management system which, among other things, identifies the foreseeable risks associated such a system and eliminate and mitigate these risks through design to the extent possible.¹⁵ They must also meet certain quality criteria for data (if they rely on it as an input), provide technical documentation before putting the system on the market, maintain records, be transparent with users so that they can make sense of the output of the system and be able to use it, and provide human oversight.¹⁶

Third, there are limited risk AI systems such as bots. The requirements for these include disclosures where AI systems are used in the context of emotional recognition and biometric categorisation.¹⁷ Finally, there are minimal risk AI systems which can undertake voluntary codes of conduct resembling those prescribed for high-risk systems.¹⁸

The latest draft of the AI Act, which includes the negotiating position adopted by the Members of the European Parliament introduces additional prohibitions on biometric systems and a set of prescriptions for generative AI such as transparency requirements and detailed summaries of copyrighted data used for training these models.¹⁹ The MEPs draft prompted scathing pushback from European industry. A hundred and fifty companies noted that the MEP’s draft would harm “European competitiveness and technological sovereignty without effectively tackling the challenges” presented by AI.²⁰

Scholars critique the EU AI Act on similar grounds. They note that the prohibitions on unacceptable AI systems may be largely ineffective because they are riddled with loopholes.²¹ Illustratively, the wording of the provisions related to manipulative systems indicates that such systems may be permitted if they do not yield individual harm – the corollary being that collective harm is not accounted for.²² In addition, many of the harms and harmful conduct identified in Act may be difficult to detect.²³ Moreover, the normative stipulations such as accuracy and robustness may be difficult to implement, particularly as, in some cases enforcement falls upon low-capacity consumer organisations.²⁴

4. Vertical AI Regulation

Compared to a horizontal approach, vertical regulation of AI targets specific problems or issues raised by different AI models in different sectors. The narrow approach deployed by vertical AI regulation may be preferable to businesses as it affords them certainty (as opposed to horizontal regulations that remain necessarily vague to preserve their wide scope).²⁵ Experts suggest vertical AI regulation is also more agile as it allows for a more direct evaluation of impact – making it easier to detect correlation and causation around regulatory design and market outcome and adjust provisions accordingly.²⁶

The drawbacks of vertical AI regulation include its reliance on coordination between agencies to harmonise obligations and minimise overlap.²⁷

a. China's Deep Synthesis Provisions

One illustration of vertical AI regulation is the People's Republic of China's Regulations on the Administration of Deep Synthesis of Internet Information Services Regulations (Deep Synthesis Provisions) entered into force on 10 January 2023.²⁸ Among other things, deep synthesis technology can be used to generate deepfakes. Deepfakes are AI-generated lookalikes. An example of a deepfake are the viral Tom Cruise deepfake videos on TikTok where the “actor” is seen in a host of different scenarios. Only the individual in the videos is not Tom Cruise, rather it is the combination of the efforts of an AI visual effects artist and an actor in a digital skin that looks exactly like Tom Cruise. While mostly famous for entertainment, deepfakes present a credible information threat that can be used to use audio-visual likenesses to carry out unlawful activities.

The scope of the law includes both generative and synthesising algorithms used to produce text and other audio-visual and virtual content.²⁹ Essentially, the Deep Synthesis Provisions set out a negative list of harms that deep synthesis service providers must guard against. Illustratively, the Deep Synthesis Provisions prohibit the use of these systems in activities harming “national security, social stability and order, and the rights and interests of others”. They bar the publication of items that subvert state power, spread fake news, and violate IP and other rights. Articles 7-20 set out a battery of prescriptions for the providers of deep synthesis systems to which include creating the capability of disclosure of deepfake content through labelling,³⁰ establishing mechanisms to dispel rumours,³¹ and carrying out real identity checks for users.³²

China's narrow approach is commendable for its specificity. However, its general approach on over-censoring information online in a bid to preserve political control is likely to hurt its generative AI ambitions. Data censorship erodes data integrity, leading to the ironic outcome of diminished reliability and quality of the AI system.³³ According to a report in the Atlantic, the Chinese government is currently grappling with this conundrum as it has made dominance in AI a top national priority but is also hard pressed to let go of a longstanding tradition of information control.³⁴ Illustratively, ERNIE, a chatbot created by Baidu (the Chinese equivalent for Google), performed so poorly in a demo that the company's shares plunged shortly after.³⁵

5. Voluntary Standards and Guidelines

Another approach to AI governance is the adoption of voluntary standards and guidelines. These can be both horizontal or vertical and are typically meant to serve as guidelines for organisational actors deploying AI systems. They may be issued by industry associations, regulators, or other standard-setting organisations and agencies.

a. TEC's Draft Standard on Fairness Assessment and Rating of AI Systems

The Telecommunications Engineering Centre (TEC) in the Indian Department of Telecommunications released a draft standards on Fairness Assessment and Rating of AI systems in December 2022.

The draft standards are meant for entities developing AI systems that may rely on the standard for self-assessment, auditors evaluating AI systems, and policymakers (and other important stakeholders) dealing with AI fairness as an issue.³⁶

The Fairness Assessment framework proposed by the TEC has a bipartite structure. The first part determines factors that lead to bias by considering typologies of bias, data, models, components, lifecycle stages, and risk.³⁷ The draft standard notes causality varies for different types of bias. Similarly, the methods used to identify and isolate bias across different types and modes of data may vary.³⁸ The idea is to triangulate through evaluation of the contributing factors to bias.

Ultimately, the Standards recommend conducting a bias assessment with a three-step approach,³⁹ which begins with assessing bias risk based on the risk spectrum and components, then determining the threshold and benchmarks for bias testing, and then finally testing for bias with metrics.

The administration of these standards is through self-certification or an independent certification. The Draft standard proposes that the auditee create a bias risk assessment based on the proposed framework, then the auditor verify the propriety of this assessment based on documents and other evidence provided by the auditee.⁴⁰

Researchers have highlighted several issues with fairness metrics. The first is that fairness metrics tend to assess the fairness of models in different ways and there is a general dearth of congruence between these metric systems.⁴¹ Consequently, one could configure a model to conform to a set of fairness metrics without considering others.⁴² The second issue is that in academic discourse is fairness is typically discussed in the context of large datasets, which raises questions about the reliability of prescribed metrics for small datasets that are often used for natural-language processing.⁴³ In fact, researchers found that “commonly accepted bias indices appear unreliable” when used on small datasets.⁴⁴ The TEC acknowledges that different metrics may have to be used to check for biases in the training data outcomes. However, the TEC Draft Standard makes no mention of the size of the dataset that it may be used on, indicating that it may have overlooked this detail.

6. Global Regulation of AI

At present, there is no global regulation of AI. However, in April 2023, digital and tech ministers from the G7 group of nations adopted the G7 Digital and Tech Ministers' Declaration. Among other things, the declaration endorsed the G7 Action Plan for enhancing global interoperability of AI governance frameworks and concurred on holding meetings on generative AI. Framework interoperability is an enduring and important theme in both the G7 as well as the G20 group of nations in digital governance. It acknowledges the global nature of digital technologies, trade, and transactions and lays the ground for harmonisation of regulatory conditions across jurisdictions. Such harmonisation smoothens cross-border digital interactions, giving enterprises legal certainty, but also limits the scope for any actors to escape oversight. As calls for the global regulation of AI grow louder,⁴⁵ it may be international groupings such as the G7 and the G20 that lead the way to developing a framework.

Another vehicle for international cooperation on AI is the Global Partnership on Artificial Intelligence (GPAI).⁴⁶ The GPAI is a multi-stakeholder initiative – bringing together civil society, industry, academia, and the public sector.⁴⁷ It seeks to support “cutting-edge research and applied activities on AI-related priorities”.⁴⁸

III. HOW TECHNOLOGY LAWS IMPACT ARTIFICIAL INTELLIGENCE

While technology laws are not enacted specifically to regulate AI, they can impact its development in significant ways. This section considers the impact of data protection and intellectual regulation on AI development and deployment.

a. Data Protection

Data protection laws such as the General Data Protection Regulation in the EU are likely to impact AI in multiple ways as the development of the technology rests on harvesting data. For entities that do not have large platforms to capture user data, collection is carried out through web crawlers, software that trawls the internet for information and systematises it, or other data scraping tools. These activities conflict with data protection laws that require persons processing personal data to do so by obtaining consent, which is not possible for entities that do not interface with users of platforms they may be scraping data from.

Beyond consent, principles such as storage limitation that require data processors to delete data once the purpose for which it was collected has been carried out would preclude the ability of firms to retain valuable training data.⁴⁹ Similarly, purpose limitation may preclude the use of data for training an AI model, if such a purpose was not specified to the data principal at the time of receiving the consent for the use of such data.⁵⁰ In such an instance, such a purpose would have to be conceived in advance of the collection and use of that data, which is not always practical or feasible as data use-cases (much like technological development) may not be foreseeable.⁵¹

An added dimension is that compliance related to laws like the GDPR requires the onboarding of additional personnel. One survey conducted by researchers at Boston University reveals that over 60 percent of firms noted that they would hire additional resources to manage GDPR compliance.⁵²

b. Intellectual Property

Artificial intelligence and IPR intersect in three key ways. The first is quite straightforward. Developers of AI are entitled to some exclusive rights over their innovations either in the form of patents or copyright. In India, under Section 3(k) of the Patents Act, 1970, computer programs per se and algorithms are not patentable as inventions. However, in the matter of *Ferid Allani vs Union of India & Ors*, the Delhi High Court observed that most innovation in today's digital world rests on computer programs and thus, it would be regressive to contend that "all such programs were not patentable". The court noted that the effect of such programs produced was "crucial" for weighing their patentability. The court noted that "if the invention demonstrates a "technical effect" or a "technical contribution" it is patentable even though it may be based on a computer program".⁵³ In the matter of *Microsoft Technology Licensing, LLC, vs The Assistant Controller of Patents and Designs*, the Delhi High Court noted that algorithms executed in a pre-defined sequential manner were not necessarily devoid of a technical effect or contribution.⁵⁴ In light of these decisions, artificial intelligence algorithms may receive patents provided they demonstrate some technical effect or contribution. However, there is a lack of clarity around such a position. Towards this end, the court

in the Microsoft Technology case noted that the patent office should issue clarificatory guidelines around software-based inventions.⁵⁵ AI algorithms can, however, be granted copyright as computer programs are deemed a literary work under the Copyright Act, 1957.

The second intersection between IP and AI is the use of data by the latter which may impinge on the former. Illustratively, generative AI can create text, images, and other audio-visual content but the basis of such content can be someone else's IP. Illustratively, in the United States, a band of artists have filed a lawsuit against companies that have released certain AI art generators, claiming that these models violate copyright as they have been trained on copyrighted images.⁵⁶ While training AI on copyrighted material for research falls within the bounds of fair-use under the Copyright Act, the commercialisation of such AI models is a legal grey area. Lawsuits around these issues may settle certain matters in years to come but it is incumbent on legislators to bring greater clarity out in the law to safeguard rightsholders while also enabling the development of unique and useful AI applications.

A third way AI and IP intersect is the ownership of IP in AI generated works. Illustratively, the 161st Report of the Department Related Parliamentary Standing Committee on Commerce on the Review of the IPR Regime in India noted states that algorithms run on AI are not patentable. There is a similar lack of clarity around copyrightable works generated by AI. In 2021, an AI art application known as "RAGHAV" was registered as a co-author of a work called "Suryast" with the Indian Copyright Office.⁵⁷ However, a year later, the Copyright Office issued a withdrawal indicating that copyright in the artistic work would vest in the artist.⁵⁸

IV. TAKEAWAYS AND CONSIDERATIONS FOR THE WAY FORWARD: BUCK THE TREND OF HORIZONTAL REGULATION

Horizontal AI regulation, which is often inspired by guidelines for ethical AI, is likely to be overly prescriptive without necessarily addressing the risks posed by different AI models. To reiterate, it often fails to distinguish between the different AI models, instead treating AI as a monolith. This may translate into the indiscriminate application of a set of regulatory principles (and provisions inspired by them) to different types of AI, even where they might have no relevance.⁵⁹ For instance, intelligent agents like robots do not present any “fairness” harms.⁶⁰ Yet, regulations such as the EU AI Act would apply provisions addressing fairness to these AI models as well.⁶¹

Scholars propound an alternative approach, where the potential harmful effects of different AI models are empirically tested and evaluated, and suitably addressed with correspondent remedial mechanisms.⁶² To some extent, vertical AI regulation tends to follow this approach, albeit many of the stipulations in China’s deep synthesis regulation are questionable from a rights and ethics perspective.⁶³ In addition, China’s proclivity for strong State control over information may reduce the competitiveness of its domestic AI endeavours.

India must work to buck the global trend of horizontal AI regulation and come out with sector-specific provisions that address the harms presented by different models. In addition, it must work to ensure that AI regulatory provisions do not undermine related policy priorities. For instance, requiring disclosure of training data can undermine security and make models more vulnerable to attacks.⁶⁴ Similarly, requiring AI training data to be error free can hinder the availability of data and reduce competitiveness in innovation.⁶⁵

In the context of addressing the intersection between AI and existing laws, India can reduce the friction between AI development and data protection by leveraging exemptions within the Digital Personal Data Protection Act, 2023. Section 17(3) of the recently enacted data protection law empowers the Government to exempt startups and other data fiduciaries from certain obligations pertaining to notice, ensuring the accuracy and completeness of personal data, and data retention restrictions.⁶⁶ This exemption could be granted to AI start-ups and other entities working on creating these systems. On intellectual property and AI, a considerable amount of work needs to be done to understand the implications of AI development for rightsholders. Greater clarity is also needed on the position under both patent and copyright law on the protections afforded to AI algorithms as well as authorship of works.

Finally, voluntary standards are an important facet of AI development. However, these must be carefully produced and well-researched if they are to have any utility.

REFERENCES

- 1 https://orfonline.org/wp-content/uploads/2018/11/Ai_Book.pdf
- 2 https://orfonline.org/wp-content/uploads/2018/11/Ai_Book.pdf
- 3 <https://www.nature.com/articles/s42256-019-0088-2>
- 4 <https://www.nature.com/articles/s42256-019-0088-2>
- 5 <https://www.nature.com/articles/s42256-019-0088-2>
- 6 <https://arxiv.org/ftp/arxiv/papers/2303/2303.11196.pdf>
- 7 <https://arxiv.org/ftp/arxiv/papers/2303/2303.11196.pdf>
- 8 <https://arxiv.org/ftp/arxiv/papers/2303/2303.11196.pdf>
- 9 <https://arxiv.org/ftp/arxiv/papers/2303/2303.11196.pdf>
- 10 <https://arxiv.org/pdf/2107.03721.pdf>
- 11 <https://arxiv.org/pdf/2107.03721.pdf>
- 12 <https://arxiv.org/pdf/2107.03721.pdf>
- 13 There are certain exceptional cases where such systems can be deployed such as the targeted search for victims of crime such as missing children, prevention of a specific and imminent threat to life of physical safety of natural persons or a terrorist attack, the detection, localization, identification or prosecution of a perpetrator or suspect of a criminal offence recognized under Article 2/2 of Council Framework Decision 2002/584/JHA
- 14 <https://arxiv.org/pdf/2107.03721.pdf>
- 15 <https://arxiv.org/pdf/2107.03721.pdf>
- 16 <https://arxiv.org/pdf/2107.03721.pdf>
- 17 <https://arxiv.org/pdf/2107.03721.pdf>
- 18 <https://arxiv.org/pdf/2107.03721.pdf>
- 19 <https://arxiv.org/pdf/2107.03721.pdf>
- 20 <https://drive.google.com/file/d/1wrtxfvcD9FwfNfWGDL37Q6Nd8wBKXCkn/view>
- 21 <https://arxiv.org/pdf/2107.03721.pdf>
- 22 <https://arxiv.org/pdf/2107.03721.pdf>
- 23 <https://arxiv.org/pdf/2107.03721.pdf>
- 24 <https://arxiv.org/pdf/2107.03721.pdf>
- 25 <https://www.holisticai.com/blog/regulating-ai-the-horizontal-vs-vertical-approach>.
- 26 <https://arxiv.org/ftp/arxiv/papers/2303/2303.11196.pdf>
- 27 *Id.*
- 28 Text available at <https://www.chinalawtranslate.com/en/deep-synthesis/>.
- 29 Article 2, <https://www.chinalawtranslate.com/en/deep-synthesis/>.
- 30 Article 14, <https://www.chinalawtranslate.com/en/deep-synthesis/>.
- 31 Article 17, <https://www.chinalawtranslate.com/en/deep-synthesis/>.

-
- 32 Article 9, <https://www.chinalawtranslate.com/en/deep-synthesis/>.
- 33 <https://arxiv.org/ftp/arxiv/papers/2303/2303.11196.pdf>
- 34 <https://www.theatlantic.com/international/archive/2023/04/chatbot-ai-problem-china/673754/>
- 35 <https://www.reuters.com/technology/chinese-search-giant-baidu-introduces-ernie-bot-2023-03-16/>
- 36 https://tec.gov.in/pdf/SDs/TEC%20Draft%20Standard%20for%20fairness%20assessment%20and%20rating%20of%20AI%20systems%20final%202022_12_27.pdf
- 37 https://tec.gov.in/pdf/SDs/TEC%20Draft%20Standard%20for%20fairness%20assessment%20and%20rating%20of%20AI%20systems%20final%202022_12_27.pdf
- 38 https://tec.gov.in/pdf/SDs/TEC%20Draft%20Standard%20for%20fairness%20assessment%20and%20rating%20of%20AI%20systems%20final%202022_12_27.pdf
- 39 Aihik Sur, “What DoT’s draft standard for measuring fairness of AI say and how the industry sees it”, available at <https://www.moneycontrol.com/news/business/what-dots-draft-standards-for-measuring-fairness-of-ai-say-and-how-the-industry-sees-it-10095671.html>
- 40 https://tec.gov.in/pdf/SDs/TEC%20Draft%20Standard%20for%20fairness%20assessment%20and%20rating%20of%20AI%20systems%20final%202022_12_27.pdf
- 41 https://tec.gov.in/pdf/SDs/TEC%20Draft%20Standard%20for%20fairness%20assessment%20and%20rating%20of%20AI%20systems%20final%202022_12_27.pdf
- 42 https://tec.gov.in/pdf/SDs/TEC%20Draft%20Standard%20for%20fairness%20assessment%20and%20rating%20of%20AI%20systems%20final%202022_12_27.pdf
- 43 https://tec.gov.in/pdf/SDs/TEC%20Draft%20Standard%20for%20fairness%20assessment%20and%20rating%20of%20AI%20systems%20final%202022_12_27.pdf
- 44 https://tec.gov.in/pdf/SDs/TEC%20Draft%20Standard%20for%20fairness%20assessment%20and%20rating%20of%20AI%20systems%20final%202022_12_27.pdf
- 45 <https://foreignpolicy.com/2023/06/20/openai-ceo-diplomacy-artificial-intelligence/>
- 46 <https://gpai.ai/about/>
- 47 <https://gpai.ai/about/>
- 48 <https://gpai.ai/about/>
- 49 [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf)
- 50 [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf)
- 51 [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf)
- 52 https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=2349&context=faculty_scholarship
- 53 <https://indiankanoon.org/doc/90686424/>
- 54 <https://indiankanoon.org/doc/52362832/>
- 55 <https://indiankanoon.org/doc/52362832/>
- 56 <https://news.artnet.com/art-world/class-action-lawsuit-ai-generators-deviantart-midjourney-stable-diffusion-2246770>
- 57 <https://www.mondaq.com/india/copyright/1284668/ai-works--the-future-of-intellectual-property-law>
- 58 <https://www.mondaq.com/india/copyright/1284668/ai-works--the-future-of-intellectual-property-law>
- 59 <https://arxiv.org/pdf/2303.11196.pdf>
- 60 <https://arxiv.org/pdf/2303.11196.pdf>
-

61 <https://arxiv.org/pdf/2303.11196.pdf>

62 <https://arxiv.org/pdf/2303.11196.pdf>

63 <https://arxiv.org/pdf/2303.11196.pdf>

64 <https://arxiv.org/pdf/2303.11196.pdf>

65 <https://arxiv.org/pdf/2303.11196.pdf>

66 https://prsindia.org/files/bills_acts/bills_parliament/2023/Digital%20Personal%20Data%20Protection%20Bill,%202023.pdf



ESYA
centre

www.esyacentre.org