Indic Pacific Legal Research LLP

Salience. Persistence. Adaptivity.

Proposal

Submitted on November 7, 2023

A NEW ARTIFICIAL INTELLIGENCE STRATEGY AND AN ARTIFICIAL INTELLIGENCE (DEVELOPMENT & REGULATION) BILL FOR INDIA

Abhivardhan
Founder & Managing Partner
Indic Pacific Legal Research

Akash Manwani
Chief Innovation Consultant
Indian Society of Artificial Intelligence and Law

Chairperson & Managing Trustee
Indian Society of Artificial Intelligence and Law

Proposal

A NEW ARTIFICIAL INTELLIGENCE STRATEGY

AND

AN ARTIFICIAL INTELLIGENCE (DEVELOPMENT & REGULATION) BILL FOR INDIA

Abhivardhan
Founder & Managing Partner
Indic Pacific Legal Research

Chairperson & Managing Trustee
Indian Society of Artificial Intelligence and Law

Akash Manwani
Chief Innovation Consultant
Indian Society of Artificial Intelligence and Law

Indic Pacific Legal Research LLP

Table of Contents

A New Artificial Intelligence Strategy for India [Proposal]

About this Proposal

India's first AI policy was presented to the world in 2018. The policy, developed by NITI Aayog, the Government of India's key policy think tank, envisioned India as the next "garage" for AI start-ups and their innovations. The focus on responsible AI has also been a priority of the G20 India Presidency. India's Council Chairpersonship of the Global Partnership on Artificial Intelligence (GPAI) in 2023 reflects the Government of India's commitment to the field of AI as an industry.

However, nearly 4-5 years have elapsed since the release of the 2018 AI policy. The technology landscape has undergone significant changes during this period. In my opinion, the current policy is no longer adequate or appropriate for the post-COVID technology market.

The rise of generative AI and Artificial Intelligence Hype has also been a challenge. This has created uncertainty for investors and entrepreneurs, hindering innovation. Many use cases and test cases of generative AI and other forms of AI applications remain scattered and uncoordinated. There is no clear consensus on how to regulate different classes of AI technologies.

While there have been some international declarations and recommendation statements through multilateral bodies/groups like UNESCO, ITU, OECD, the G20, the G7, and the European Union, even the UN Secretary General has stressed the need for UN member-states to develop clear guidelines and approaches on how to regulate artificial intelligence in his 2023 UN General Assembly address.

This proposal submitted by **Indic Pacific Legal Research** addresses those key technology, industry and legal-regulatory problems and trends, and presents a **point-to-point proposal** to

reinvent and develop a revised National Strategy on Artificial Intelligence. The proposal consists of a set of law & policy recommendations, with a **two-fold approach**:

- The Proposal for a Revised National Strategy for Artificial Intelligence
- The Proposal for the Artificial Intelligence (Development & Regulation) Act, 2023

In the Annex to this Proposal, we have provided additional Recommendations on Artificial Intelligence Policy based on the body of research developed by **Indic Pacific Legal Research** and its member organizations, including, the **Indian Society of Artificial Intelligence and Law**.

About Us

Indic Pacific Legal Research has been delivering on pioneering innovation in legal and policy research, with an Indian and global overview, since 2019. Our notable initiatives include the Indian Society of Artificial Intelligence and Law and Global Law Assembly.

Indic Pacific is an emerging technology law consultancy, which delivers its consulting services in the areas of **law**, **technology** and **global governance**.

Website | **indicpacific.com**

About the Authors

Abhivardhan is honoured to serve as the **Chairperson & Managing Trustee** of the **Indian Society of Artificial Intelligence and Law** and as the **Managing Partner** at **Indic Pacific Legal Research**. Throughout his journey, he has gained valuable experience in **international technology law, corporate innovation, global governance, and cultural intelligence**.

With deep respect for the field, Abhivardhan has been fortunate to contribute to esteemed law, technology, and policy magazines and blogs. His book, "**Artificial Intelligence Ethics and International Law: An Introduction**" (2019), modestly represents his exploration of the important connection between artificial intelligence and ethical considerations. Emphasizing the significance of an Indic approach to AI Ethics, Abhivardhan aims to bring diverse perspectives to the table.

Abhivardhan remains humbled by the opportunity to share knowledge through various papers on international technology law. Alongside his consulting and policy advocacy, he has been involved in both authoring and editing books, focusing on public international law and its relationship with artificial intelligence. Some of his notable works also include the **2020 Handbook on AI and International Law**, the **2021 Handbook on AI and International Law** and the technical reports on **Generative AI, Explainable AI and Artificial Intelligence Hype**.

Akash Manwani is honoured to serve as the Chief Innovation Consultant of the Indian Society of Artificial Intelligence and Law. His work embodies a fusion of legal rigor and forward-thinking, positioning him as a vital voice in shaping the dialogue around artificial intelligence in the legal sphere. His notable works include *2020 Handbook on AI and International Law* and Technical Reports on *AI Auditing* and *Web3*.

Acknowledgments

We express our gratitude to the research team of **Indic Pacific Legal Research** for their dedication in drafting and formulating this full-fledged proposal:

Bhavana J Sekhar
Principal Researcher

Sanad Arora
Senior Research Associate

In the initial rounds of development of the proposal, this proposal was discussed and deliberated in the *AI General Assembly R&D Committee*, a forum of technology law and policy specialists and researchers, and the *Advisory Council* of the **Indian Society of Artificial Intelligence and Law**.

We are grateful for the insights and moral support of the Distinguished Experts of the Advisory Council:

Sanjay Notani
President, AI General Assembly
Partner, Economic Laws Practice, India

Bogdan Grigorescu
Vice-President, AI General Assembly
Senior Technical Lead - Architecture, eBay, United Kingdom

Shirsha Ray Chaudhari
Director of Engineering, TR Labs, Thomson Reuters, India

We are grateful for the insights and moral support of the members of the *AI General Assembly R&D Committee*:

A New Artificial Intelligence Strategy for India [Proposal]

Pavithra Manivannan, Chairperson of the Committee
Rishabh Bezbaruah
Tushar Sharma
Hari Shivan
Samridhi Jain
Kailash Chauhan
Indrasen Poola

A New Artificial Intelligence Strategy for India [Proposal]

Background

To provide a concise overview of the state of 'AI Ethics' both globally and in India, it is crucial to focus on three key domains: **(1) technology development and entrepreneurship**, **(2) industry standardization**, and **(3) legal and regulatory matters**. Our organization has actively contributed to this field by producing significant reports and publications that highlight critical issues related to AI regulation and address the prevailing hype around AI. These contributions are detailed below for your further review and consideration.

- 2020 Handbook on AI and International Law [RHB 2020 ISAIL]
- Regulatory Sovereignty in India: Indigenizing Competition-Technology Approaches, **ISAIL-TR-001**
- Regularizing Artificial Intelligence Ethics in the Indo-Pacific, GLA-TR-002
- 2021 Handbook on AI and International Law [RHB 2021 ISAIL]
- Regulatory Sandboxes for Artificial Intelligence: Techno-Legal Approaches for India, **ISAIL-TR-002**
- Deciphering Artificial Intelligence Hype and its Legal-Economic Risks, **VLiGTA-TR-001**
- Deciphering Regulative Methods for Generative AI, **VLiGTA-TR-002**

- Promoting Economy of Innovation through Explainable AI, **VLiGTA-TR-003**

Technology Development and Entrepreneurship

- Investors express apprehension regarding the widespread adoption of AI applications and the absence of technological neutrality required for ensuring their long-term sustainability across various products and services. In order to foster an environment conducive for MSMEs and emerging start-ups to embark on AI research and the development of AI solutions, it is imperative to provide them with subsidies.
- Currently, India faces a deficiency in the requisite ecosystem for AI endeavours. Even prominent semiconductor firms like NVIDIA and major technology entities such as Reliance and TCS have advocated for government support in semiconductor investments and the establishment of robust computing infrastructure to benefit local start-ups.

Industry Standardisation

- As prominent companies actively establish their own Responsible AI guidelines and self-regulatory protocols, it becomes imperative for India to prioritize the adoption of industry standards for the classification and categorization of specific use cases and test cases. We had previously proposed this approach in the context of Generative AI applications in a prior document.
- The application of AI technology in Indian urban and rural areas, spanning various sectors, naturally involves elements of reference and inference unique to the region. However, it is noteworthy that the predominant discourse on 'AI ethics'

has been primarily confined to major cities such as New Delhi and a select few metropolitan centers. In order to facilitate the development of AI policies, AI diplomacy, AI entrepreneurship, and AI regulations – the four essential facets of India's AI landscape, it is imperative to ensure the active participation and equitable recognition of stakeholders from across the country.

- Distinguished industry and policy organizations, although representing the concerns of larger players including prominent names, are fulfilling their expected role. Nonetheless, relying solely on these entities to devise, propose, and advocate solutions tailored to the requirements of our MSMEs and emerging start-ups could potentially hinder the establishment of industry-wide standards. Therefore, the Ministry of Electronics and Information Technology (MeiTY) should engage in thoughtful collaboration with the Ministry of Commerce & Industry to address the issue of gatekeeping within the AI sector across the **four domains of AI policy, AI diplomacy, AI entrepreneurship, and AI regulation**.

Legal and Regulatory Issues

- Many use cases and test cases of AI applications as products and services, across industry sectors lack transparency in terms of their commercial viability and safety on even basic issues like data processing, privacy, consent and right of erasure (dark patterns). At the level of algorithmic activities and operations, there is a lack of sector-specific standardisation, which could be advantageous for Indian regulatory authorities and market players in driving policy interventions & innovations at a global level. Nevertheless, the best countries can do is to have their regulators enforce existing **sector-specific regulations** to test and enable better AI regulation standards, starting from data protection

& processing to the issue of algorithmic activities & operations.

- In a global context, it's worth noting that think tanks, as well as prominent AI ethics advocates and thought leaders in Western Europe and Northern American nations, exhibit comparatively lesser interest in the G20's efforts to advance Responsible AI ethics standards. Their attention appears to be primarily drawn to the Responsible AI principles and solutions emerging from the G7 Hiroshima, a perspective that is duly acknowledged.

- However, it is noteworthy that a significant number of AI ethicists and industry figures in Western Europe and Northern America seem to be overlooking the valuable contributions and viewpoints that India offers in the realm of AI Ethics.

- Moreover, it is essential to recognize that vital stakeholders responsible for advancing discussions on AI ethics and policy within South East Asia (comprising ASEAN nations) and Japan have similarly overlooked the ongoing AI policy discourse in India. Given India's dedication to establishing the Indo-Pacific Quad—a partnership encompassing India, Australia, the United States, and Japan—with the aim of fostering collaboration on pivotal technologies and regulatory matters, it is imperative for the Government of India to take significant steps to facilitate cooperation with dedicated and relevant AI ethics industry leaders and thought leaders in South East Asia. This collaborative effort can play a crucial role in advancing the shared objectives of the Quad.

- The discourse surrounding AI and Law in India has largely remained unchanged without any notable developments or transformative shifts. The predominant topics of discussion

have primarily revolved around issues related to data protection rights, notably exemplified by the introduction of the **Digital Personal Data Protection Act, 2023**. Additionally, considerations have also extended to address concerns related to information warfare and sovereignty and develop a civil & criminal liability regime for digital intermediaries, a notable instance being the introduction of the **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**.

- Nevertheless, it is laudable to observe that at the level of the Council of Ministers, there exists a discernible and unwavering commitment to driving forward these discussions. This unwavering intent reflects a dedicated approach towards addressing the intricate convergence of AI and legal aspects in the Indian context.

- Indeed, legislative advancements in areas like **digital sovereignty**, **digital connectivity**, **drones**, **dark patterns** and **data protection** & **consent** have been both **responsive** and **aligned** with the needs of the Indian legal landscape. On numerous intricate facets of law and policy, there is no pressing urgency for regulatory interventions in India. However, a notable observation is the absence of original thinking and innovative insights focused on technology law and policy within the country.

- The discourse surrounding AI and Law within India tends to be confined to addressing three primary issues:

    - **Digital sovereignty**
    - **Data protection law**
    - **Responsible AI**

- With the exception of the first two concerns, it becomes apparent that documents published by various entities involved in AI policy have been somewhat inadequate in fostering an informed, industry-specific approach towards regulating and nurturing a thriving AI sector in India.

- Despite the Government's expressed commitment to encouraging policy inclusivity, a significant hurdle has been the prevalence of gatekeeping practices across the landscape of law and policy influencers and thought leaders. Regrettably, many of these discussions tend to gain recognition and significance only when conducted in a handful of major metropolitan areas, thus limiting the diversity and inclusivity of perspectives.

- Numerous AI companies in India have yet to establish standardized **self-regulatory frameworks** aimed at **fostering market integrity**. This situation can be attributed to a confluence of factors.

    - **First**, the proliferation of use cases is essential to stimulate the adoption of self-regulatory practices and measures.

    - **Second**, even if the commercial need for self-regulation is acknowledged, the absence of significant advancements in the AI and Law discourse in India for nearly 4-5 years has resulted in a lack of clarity concerning the country's stance on four critical dimensions: AI policy, AI diplomacy, AI entrepreneurship, and AI regulation. This lack of clarity contributes to regulatory uncertainty, akin to the challenges faced by the Web3 and gaming industries in India.

- **Third**, this lack of clarity in policy and regulation creates an environment of uncertainty, similar to the issues faced by the Web3 and gaming industries in India.

- **Fourth**, gatekeeping practices further compound the complexity of the discourse and hinder the engagement of diverse voices. This sentiment is echoed by key commercial players across strategic & non-strategic and emerging sectors in India, highlighting the need for a more inclusive and open dialogue.

The Proposal for a New AI Strategy for India

Proposal for a New Artificial Intelligence Strategy for India

We suggest that in a reinvented AI strategy for India, the four pillars of India's position on Artificial Intelligence must be **AI policy, AI diplomacy, AI entrepreneurship** and **AI regulation.** These are the most specific commitments in the four key areas that could be achieved in **5-10 years**. The rationale and benefits of adopting each of the points in the policy proposal are explained on a point-to-point basis.

AI Policy

#1

Strengthen and empower India's Digital Public Infrastructure to transform its potential to integrate governmental and business use cases of artificial intelligence at a whole-of-government level.

Proposition	Rationale & Benefits
Whole-of-government approach	A whole-of-government approach to AI is essential for ensuring that AI is used effectively and efficiently across government. This requires coordination and collaboration between different government agencies. Such an approach to AI can help to avoid duplication of effort, ensure consistency of approach, and maximize the benefits of AI in a flexible and coordinated manner.

#2

Transform and rejuvenate forums of judicial governance and dispute resolution to keep them effectively prepared to address and resolve disputes related to artificial intelligence, which are related to issues ranging from those of data protection & consent to algorithmic activities & operations and corporate ethics.

Proposition	Rationale & Benefits
Effective preparedness of courts, tribunals and dispute resolution forums	Forums of judicial governance and dispute resolution play a crucial role in ensuring that AI is used in a fair and just manner. These forums provide a platform for individuals and businesses to seek redress in the event of disputes related to AI. It would become necessary for the courts, tribunals and dispute resolution forums to address the interpretability and maintainability of technology law disputes, at various levels, as proposed: • *Level 1*: Data Protection / Privacy / Consent / Processing Issues • *Level 2*: Level 1 + Sector-specific Civil Law Issues • *Level 3*: Algorithmic Use and Ethics Issues • *Level 4*: Level 3 + Issues related to AI Governance in Companies / Government Bodies • *Level 5*: AI and Corporate Practice Issues + Sector-specific Competition Law / Trade Law / Investment Law Issues • *Level 6*: Level 5 + Telecom Arbitration / Technology Arbitration
Reasonable Distinction of	For courts, tribunals and dispute resolution forums to address and resolve disputes related to

Legal and Policy Issues

artificial intelligence and law, they would require to adopt a technology-neutral approach to interpret and examine the veracity of legal issues related to artificial intelligence use, proliferation and democratisation, based on a reasonable distinction of legal and policy issues, as proposed:

- Data Protection / Privacy / Consent Issues
- Data Processing and Pseudonymisation Issues
- Legitimate Use of Data-related Issues
- Data Erasure / Right to be Forgotten Issues
- Contractual Disputes between Data Processors, Consumers and Data Fiduciaries
- Jurisdiction and Cross-Border Ownership and Liability Questions
- Transboundary Flow of Data
- Algorithmic Ethics Issues in Company Law
- Algorithmic Transparency and Bias Issues in Commercial Law
- Regulation and Compliance of Algorithmic Activities & Operations of AI Use Cases, subject to their Technical Features and Commercial Viability
- Artificial Intelligence Governance Issues at Business-to-Business & Business-to-Government levels.
- AI-related Mergers & Acquisitions Issues
- AI-related Investment Issues
- Arbitrability of Telecom Disputes Arising out of use of Artificial Intelligence Technologies

AI Diplomacy

#3

Focus on the socio-technical empowerment and skill mobility for businesses, professionals, and academic researchers in India and the Global South to mobilize and prepare for the proliferation of artificial intelligence & its versatile impact across sectors.

Proposition	Rationale & Benefits
Provide training and education on AI preparedness	Educate businesses, professionals, and academic researchers in India and Global South to strengthen them for preparedness against the risks and proliferation of artificial intelligence technologies.
Promote AI adoption	Enable AI learning and mobilization among businesses, professionals and academic researchers beyond preparedness to enable them to adopt and utilise relevant AI use cases. This helps them to help regulators in India and Global South countries to develop reasonable compliance frameworks and industrial standardisation ecosystems.

#4

Enable safer and commercially productive AI & data ecosystems for startups, professionals and MSMEs in the Global South countries.

Proposition	Rationale & Benefits
Enable Safer AI & Data Ecosystems	• Aid start-ups, professionals, and MSMEs in the Global South to navigate the complexities of AI with confidence and security.

	• Promote risk mitigation, ensuring that these entities can explore AI and data-driven ventures without excessive threats to their businesses. • Foster innovation by creating an environment where start-ups, professionals, and MSMEs can experiment with AI solutions, driving economic growth. • Encourage foreign and domestic investments, positioning the Global South as an attractive hub for AI entrepreneurship and development.

#5

Bridge economic and digital cooperation with countries in the Global South to promote the implementation of sustainable regulatory and enforcement standards, when the lack of regulation on digital technologies, especially artificial intelligence becomes an unintended systemic, economic and political risk.

Proposition	**Rationale & Benefits**
Bridge Economic and Digital Cooperation to Promote Sustainable Regulatory and Enforcement Standards	• Address the inherent risks posed by the absence of regulations on digital technologies, reducing systemic, economic, and political vulnerabilities. • Encourage knowledge exchange and best practices sharing among nations, enabling the implementation of sustainable regulatory and enforcement standards for AI and digital technologies. • Enhance the digital readiness of Global South countries, positioning them to tap into the opportunities presented by AI while mitigating risks and uncertainties.

- Strengthen diplomatic and economic relationships, creating a mutually supportive environment for nations as they navigate the complexities of AI and digital ecosystems.
- Position the Global South as a collective force in shaping AI regulations and standards, allowing its members to have a more influential and balanced role in the global AI landscape.

AI Entrepreneurship

#6

Develop and promote India-centric, locally viable commercial solutions in the form of AI products & services.

Proposition	Rationale & Benefits
Promote innovation and economic growth	Developing and promoting India-centric, locally viable commercial solutions in the form of AI products and services can help to promote innovation and economic growth. AI-powered products and services can create new jobs, boost productivity, and open up new markets.
Encourage the development of locally viable AI solutions in India	This can help to reduce India's reliance on foreign technology. This can make India more resilient to external shocks and give it more control over its own economic destiny.

#7

Enable the industry standardization of sector-specific technical & commercial AI use cases.

Proposition	**Rationale & Benefits**
Enable Industry Standardization	• Promote consistency and interoperability in AI applications across sectors, reducing fragmentation and enhancing efficiency. • Foster the development of clear benchmarks for AI use cases, facilitating seamless integration and promoting fair competition • Position India to lead in sector-specific AI use cases, attracting investments and fostering innovation in targeted industries • Empower professionals and businesses by offering a structured approach to AI adoption, reducing barriers to entry and risks associated with uncertainty.

#8

Subsidize & incentivize the availability of compute infrastructure, and technology ecosystems to develop AI solutions for local MSMEs and emerging start-ups.

Proposition	**Rationale & Benefits**
Provide financial assistance to SMEs and start-ups to purchase cloud computing resources	Provide financial assistance to SMEs and start-ups to purchase cloud computing resources, such as compute power, storage, and networking. This will make it more affordable for SMEs and start-ups to access the resources they need to develop and deploy AI solutions.

Establish AI innovation hubs	Establish AI innovation hubs across the country. These hubs will provide SMEs and start-ups with access to compute infrastructure, technology ecosystems, and expertise. The hubs can also help to foster collaboration between SMEs, start-ups, and other stakeholders.
Partner with universities and research institutions	Partner with universities and research institutions to develop AI curriculum and to provide training to SMEs and start-ups on AI. This will help to ensure that SMEs and start-ups have the skills and knowledge they need to develop and deploy AI solutions.

#9

Establish a decentralized, localized & open-source data repository for AI test cases & use cases and their training models, with services to annotate & evaluate models and develop a system of incentives to encourage users to contribute data and to annotate and evaluate models.

Proposition	Rationale & Benefits
Establish Decentralized Data Repository	• Facilitate accessibility to AI test cases, use cases, and training models, promoting transparency and innovation within the AI ecosystem on a sector-wide basis. • Encourage the development of localized, context-aware AI solutions that are adapted to the nuances and requirements of different regions and communities. • Foster open-source collaboration, allowing AI practitioners and developers to contribute, annotate, and evaluate models, enhancing knowledge sharing and the quality of AI systems.

- Enhance the quality of AI models through crowdsourced annotation and evaluation, leading to better-performing, more reliable AI applications.
- Establish a system of incentives to motivate users to actively participate in data contribution, annotation, and evaluation, creating a collaborative AI ecosystem.
- Supports the development of AI solutions that align with local requirements and cultural sensitivities, fostering the ethical and responsible deployment of AI.

#10

Educate better and informed perspectives on AI-related investments on areas such as:

(1) research & development,
(2) supply chains,
(3) digital goods & services and
(4) public-private partnership & digital public infrastructure.

Proposition	Rationale & Benefits
Research & Development	Ensure that stakeholders are well-informed about AI investments in research and development, promoting effective allocation of resources.
Supply Chains	Enhance the understanding of AI's impact on supply chains, optimizing logistics and creating resilience in the face of disruptions.
Digital Goods & Services	Promote informed investment in the development of digital goods and services, aligning product offerings with market needs and emerging trends.

Public Private Partnership & Digital Public Infrastructure	Facilitate the creation of robust public-private partnerships, fostering collaboration to develop digital public infrastructure that benefits society. The potential of public-private partnerships to boost the use and proliferation of India's DPI remains untapped and AI education can address the gaps.

#11

Address and mitigate the risks of artificial intelligence hype by promoting net neutrality to discourage anti-competitive practices involving the use of AI at various levels and stages of:

(1) research & development,
(2) maintenance,
(3) production,
(4) marketing & advertising,
(5) regulation,
(6) self-regulation, and
(7) proliferation.

Proposition	**Rationale & Benefits**
Research & Development Stage	Encourage fair competition in AI research and development, preventing undue concentration of power and resources.
Stages of Maintenance, Production, Marketing, and Advertising	Reduce the risk of AI maintenance, production, marketing, and advertising becoming platforms for hype, ensuring ethical and responsible AI promotion.
Stages of Regulation, Self-Regulation and Proliferation	Mitigate the risk of AI proliferation without proper oversight, ensuring that AI technologies are developed and utilized responsibly and for the greater good.

AI Regulation

#12

Foster flexible and gradually compliant data privacy and human-centric explainable AI ecosystems for consumers and businesses.

Proposition	Rationale & Benefits
Foster flexible and gradually compliant data privacy and human-centric explainable AI ecosystems for consumers and businesses.	A flexible and gradually compliant approach to data privacy and AI regulation can help to address these challenges while also promoting innovation. This can ensure: • Reduced risk of harm from AI systems • Increased customer trust • Enhanced reputation

Specific legal and policy issues for consideration

Data Protection / Privacy / Consent Issues	Ensure the sector-neutral interpretative and adjudicatory enablement of data protection rights, and enforcement mechanisms in line with the Digital Personal Data Protection Act, 2023 & its guidelines and the Code of Civil Procedure, 1908.
Data Processing and Pseudonymisation Issues	It is important to ensure that data is processed in a fair and explainable manner and that pseudonymisation is used where appropriate to protect the privacy of individuals.
Legitimate Use of Data-related Issues	The legitimate use of personal and non-personal data must be clarified, standardized

	and sensitized by the efforts of regulatory, judicial & dispute resolution institutions.
Data Erasure / Right to be Forgotten Issues	Consumers have the right to have their data erased in certain circumstances. There will be legible consumer law, and competition law issues, where the lack of abiding by the right to be forgotten generates dark patterns, which need to be adequately dealt with.
Contractual Disputes between Data Processors, Consumers and Data Fiduciaries	AI systems often involve complex contractual relationships between data processors, consumers, and data fiduciaries. It is important to ensure that these contracts are clear and fair and that consumers have access to effective dispute resolution mechanisms.
Algorithmic Ethics Issues in Company Law	AI systems can raise a number of algorithmic ethics issues. It is important to develop company law principles that promote the responsible & explainable use of AI.
Algorithmic Transparency and Bias Issues in Commercial Law	AI systems can often be opaque and difficult to understand. It is important to develop commercial law principles that promote transparency and accountability in AI systems.

#13

Develop regulatory sandboxes for sector-specific use cases of AI to standardize AI test cases & use cases subject to their technical and commercial viability.

Proposition	Rationale & Benefits
Standardization of AI test cases and use cases via regulatory sandboxes	*Regulatory sandboxes* can provide a safe and controlled environment for testing and evaluating AI applications in a sector-specific context. For example, a *regulatory sandbox* could be established to allow healthcare providers and technology companies to test and evaluate AI-powered medical diagnostic tools. This would involve developing a set of standardized test cases and use cases that could be used to assess the *accuracy*, *safety*, and *efficacy* of these tools.
Improving technical and commercial viability of AI applications	Regulatory sandboxes can help to identify and address the *regulatory* and *commercial challenges* associated with the *deployment* of AI applications. This can help to make AI applications more *technically* and *commercially viable*, and to accelerate their adoption. In addition, defining human autonomy and its extent for AI use cases, technical & commercial, could be helpful for research and commercial purposes, to further standardise AI in the context of the future of work & innovation.

#14

Promote the sensitization of the first order, second order and third order effects of using AI products and services to B2C consumers (or citizens), B2B entities and even inter and intra-government stakeholders, which includes courts, ministries, departments, sectoral regulators and statutory bodies at both standalone & whole-of-government levels.

Proposition	Rationale & Benefits
Sensitization for B2C Consumers	This would be helpful to inform consumers to be vigilant against market practices, which reveal dark patterns and other forms of manipulative practices engineered and promoted through artificial intelligence systems.
Sensitization for B2B entities	To help businesses make informed decisions about the use of AI in their businesses and to enhance their competitiveness.
Sensitization for inter and intra-government stakeholders	To maintain and improve the trust quotient of inter and intra-government stakeholders at two levels: • For standalone government and judicial institutions • For all organs of the government, from the judicial institutions to the executive branches, which includes statutory, cooperative, diplomatic and administrative sections of the Government of India, and the

	administrative branches of various state and union territory governments.

#15

Enable self-regulatory practices to strengthen the sector-neutral applicability of the Digital Personal Data Protection Act, 2023 and its regulations, circulars and guidelines.

Proposition	**Rationale & Benefits**
Sector-neutral applicability of the Digital Personal Data Protection Act, 2023 and its regulations, circulars and guidelines.	Self-regulatory practices can also help to ensure that the Act is applied in a sector-neutral manner, meaning that it applies to all organizations, regardless of their sector of activity.

#16

Promote and maneuver intellectual property protections for AI entrepreneurs & research ecosystems in India.

Proposition	**Rationale & Benefits**
Promote IP Protections for AI Entrepreneurs in India	• Encourage AI innovation by safeguarding intellectual property rights, providing creators with a competitive advantage. • Promotes collaboration between academia, industry, and government, resulting in knowledge-sharing and cross-pollination of ideas.

Maneuver IP Protections for AI Entrepreneurs in India

- Foster a thriving AI research ecosystem by protecting inventors' discoveries, fostering a culture of creativity and entrepreneurship.
- Boost economic development by enabling AI start-ups and entrepreneurs to monetize their innovations and create revenue streams.

Based on the points of this proposal, an additional proposal for the Artificial Intelligence (Development & Regulation) Act, 2023 is provided in the next section.

The Proposal for the Artificial Intelligence (Development & Regulation) Act

We propose the creation of an **Artificial Intelligence (Development & Regulation) Act**, on the basis of the proposal for a Reinvented AI Strategy.

Purpose of the Legislation

There are legitimate legal and policy reasons to create and table an **Artificial Intelligence (Development & Regulation) Bill**. As of now, the Government of India has proposed a set of frameworks, to regulate the use and processing of personal, and non-personal data. The list of such frameworks includes:

- *Digital Personal Data Protection Act, 2023*
- *The Information Technology Act, 2000, to be replaced by a proposed Digital India Act*
- *Draft Indian Telecommunications Bill, 2022*
- *Draft Non-Personal Data Governance Framework*
- *Relevant rules and guidelines within the ambit of the DPDPA and the IT Act*

However, these frameworks, are insufficient in comparison to the increased need to have an Artificial Intelligence legislation.

In the forthcoming sections of this chapter, we have outlined **inferences** based on government documents, the international regulatory landscape of AI technologies and the recommendations offered in the body of research developed by **Indic Pacific Legal Research**, and the **Indian Society of Artificial Intelligence and Law**.

Inferences from the IndiaAI Expert Group Report, First Edition (2023)

#1 - Intellectual Property-related Considerations

- **Lack of Clarity on Joint Ventures' IP Ownership**: The Report does not clearly define how intellectual property (IP) ownership will be shared in joint ventures. This ambiguity should be addressed to prevent future disputes between the **Center of Excellence (CoE)** and industry partners.
- **Safeguarding Student Entrepreneurs and Start-ups**: While the licensing agreement model may suit student entrepreneurs and start-ups with early-stage innovations, it's crucial to protect them from potential exploitation by industry partners. The CoE should assist these entities in negotiating fair terms within the licensing agreement.
- **The Need to Ensure a Transparent IPR Determination Process**: The proposal suggests that the specific intellectual property rights (IPR) model will be decided on a case-by-case basis in consultation with the Governing Council. It's essential to ensure transparency and fairness in this process. The CoE should establish clear criteria for determining the IPR model and make this information available on its website.

Inferences

Now, on determining an IPR Model in various forms, a *spatial approach* would be needed by the Governing Council to determine the workflow of considerations on the ownership, royalties, and transferability of IPs of artificial intelligence technologies. There are going to be two major considerations, which would shape these considerations to be decided on a piecemeal basis – (1) technical features and (2) commercial viability**. This could be clearly addressed in an AI Regulation at a definitive basis.**

On **technical features**, we recommend that examining the limits of an artificial intelligence use case or test case should be the larger policy basis to procreate and encourage the development of an IPR Model, for the CoEs. The novelty of these use cases and test cases would require serial protections in the form of trademarks, industrial designs, integrated circuit-related IP protections, and even patenting. On issues of **commercial viability** and related after-effects of IPR Models on the market, the reliability of an AI use case must be taken into consideration to suggest a better IPR Model. **In a technology-neutral AI Regulation, such considerations could be included, with a sense of understanding.**

S.No	Evaluation Category	Evaluation Parameters
1	Sectoral focus and research priorities	- Assessment of the relevance of sectoral focus and research priorities in the identified application sector(s) - Assessment of the scalability and sustainability of the CoE's priorities to address critical challenges in chosen sectors - Evaluation of the potential societal impact of CoE's research findings and applications in identified sectors.

Figure 1: Sectoral Focus and Research Priorities, depicted as one of the evaluation categories in the Annexure C in the section for Working Group 1 in the IndiaAI Expert Group Report, 1st Edition (2023), page 24.

Now, it must be examined if the use case of AI system itself, is **multivariant, fungible** and **disruptive**. We recommend this considering the **Annexure C** in the section for Working Group 1, in which a template for the submission of a detailed proposal is provided with relevant caveats. The excerpt (**Figure 1**) from the **Evaluation Parameters** of the Annexure is provided for reference. The template's first parameter focuses on the sectoral value of an AI use case or system per se, which infers to the need to address technical considerations and commercial viability issues of any use case relatable to the AI application sector(s).

In addition, here is an excerpt from *Deciphering Regulative Methods for Generative AI, VLiGTA-TR-002 (2023),* a key technical report by our firm in which we have provided an approach to examine an AI use case to be multivariant, fungible and disruptive, which could be helpful:

- Classify the following – **products, services, use cases and test cases**.
- For a product, service, use case or test case to be considered **multivariant**, it must have a multi-sector impact. The multi-sector impact could be disruption of jobs, work opportunities, technical & industrial standards and certain negative implications, such as human manipulation.
- For a product, service, use case or test case to be considered **fungible**, it must transform its core purpose by changing its sectoral priorities (like for example, a generative AI product may have been useful for the FMCG sector, but could also be used by companies in the pharmaceutical sector for some reasons). Relevant legal concerns could be whether the **shift disrupts** the previous sector, or is causing collusion or is disrupting the new sector with negative implications.
- For a product, service, use case or test case to be **disruptive**, it must affect the **status quo of certain industrial and market practices** of a sector. For example, maybe a generative AI tool could be capable of creating certain work opportunities or rendering them dysfunctional for human employees or freelancers. Even otherwise, the generative AI tool could be capable in shaping work and ethical standards due to its intervention.

- Beyond these three parameters, the products, services, use cases and test cases must be tested and it should be checked if they have a **shelf-life** (say **6-12 months**) to be considered legible.
- While licensing product and service classifications must be done under national-level industry standards, specific codes could be created for generative AI applications considering the level of human oversight.
- There should be two kinds of product and service classifications provided if possible – **single-tier and multi-tier or nested**. Single-tier types are such classifications, which are ordinarily offered to any product or service. Multi-tier types represent more than one industry classification based on two factors:
    - **Level of human oversight involved in each product / service.**
    - **Subordinate or equivalent relationship of two or more product / service classifications**

A technology-neutral Artificial Intelligence Regulation should also address the following considerations as described:

- The CoE should establish a clear policy regarding IP ownership in joint ventures, developed in consultation with the Governing Council, and make it accessible on the CoE's website.
- The CoE should support student entrepreneurs and start-ups in negotiating licensing agreement terms with industry partners, including providing access to legal guidance and mentorship.

- The CoE should devise a transparent and equitable process for determining the IPR model on a case-to-case basis, with clear criteria published on its website.
- The Governing Council must consider developing a separate policy understanding for open-source solutions, involving the research & development, use and proliferation of artificial intelligence technologies, and ponder this issue, whether open-source technologies must be subject to certain IPR protections or restrictions within the scope of the CoEs.

In our view, all of the issues related to intellectual property commercialization, governance and development related to artificial intelligence technologies, has to be addressed in a separate, standalone AI Regulation.

#2 – Tangible Quantifiable Yearly Outputs of the NDMO

While the **IndiaAI Expert Group Report, 1st Edition (2023)** does espouse the establishment of an India Dataset Platform (IDP) and a National Data Management Office, the policy targets of the NDMO for a period of **18 months** and so do not essentially focus on AI regulation.

Short-Term (2months)	Short-medium term (1-6 months)	Medium-Term (3-18 months)	Long-Term (18+months)
- Establishment of the National Data Management Office - Hiring of personnel to staff DMUs - Setting up of DMUs in Ministries/ Departments - Preparation of Data Strategy by DMU for the Ministry/ Department	- Publish meta-data standards & data quality standards (Phase 1) - Issue Data Identification & Classification Framework - Issue Guidelines for disclosure norms - Launch of India Datasets Platform - Launch of India Datasets Program - Draft guidelines for the creation of searchable data inventories at the Ministries/ Departments level. - Finalise schedule for curated datasets to be contributed to India Datasets Programme and uploaded to India Datasets Platform.	-Issue Data Access & Licensing Agreements -Publish Data Anonymisation Guidelines - Publish standards Meta-Data & Data Quality Standards (Phase 2)	-Publish standards & principles for Fair & Ethical Use of Data

Figure 2: Tangible Quantifiable Yearly Outputs / Targets for the National Data Management Office as per the IndiaAI Expert Group Report, 1st Edition (2023).

It is truly appreciative that the NDMO will be subject to enabling data quality standards, which will affect the way ethical standards are developed to keep a check on artificial intelligence systems and make them industrially viable, and safe. In fact, in the list of **Tangible Quantifiable Yearly Outputs / Targets** as we observe, there are certain measures within the scope of data-related legal management & operations, which are appreciated:

- *Publish meta-data standards and data quality standards (Phase 1)*
- *Issue Data Identification & Classification Framework*
- *Issue Guidelines for Disclosure Norms*
- *Draft Guidelines for the Creation of Searchable Data Inventories at the Ministries / Departments Levels*

- *Issuance of Data Access & Licensing Agreements*
- *Publication of Data Anonymization Guidelines*
- *Publish standards & principles for Fair and Ethical Use of Data*

Now, a glance at each of these measures explains why an overarching corpus of AI regulation is not proposed as of now:

1. The mandate NDMO itself is limited to data quality, processing and management issues. It is yet to be cleared as to which aspects of personal and non-personal data will be properly managed, and not regulated. Thus, achieving the measures as stated above, could be an appreciative and constructive approach forward.
2. The data processing agreements will reflect upon any company's AI ethics practices, which develops an AI system. So we can say this is a **technology-neutral backend-based approach** to regulate AI using data management practices, at least for non-personal data.
3. The key, emerging and middle-level AI and tech market players, have not been able to develop self-regulatory Explainable AI or Responsible AI guidelines as of now. In addition, it would be a huge travesty for India to copycat and adopt to regulatory and ethical standards on AI (algorithmic activities & operations) which are based on Western or American or Anglophone standards.

Here is our legal estimation (in the form of a table) of the list of **Tangible Quantifiable Yearly Outputs / Targets** as to how they could pave the need to have an AI Development & Regulation Bill.

Tangible Quantifiable Yearly Outputs	Benefits of these Outputs to enable AI Regulation
Publish meta-data standards and data quality standards (Phase 1)	Helps to ensure that data is collected and stored in a consistent and structured manner to define and access scenarios and use cases for artificial intelligence technologies.

Inference

Encourage a **phased approach to publishing meta-data and data quality standards**, which initially affect the most critical datasets for AI development in India.

They could be related to India's key strategic sectors, and fine-tuned to India's needs to incentivise its ecosystem of Digital Public Infrastructure, especially in fields like *FinTech*, *Digital Commerce*, *Agriculture*, *Governance and others*.

Issue Data Identification & Classification Framework	Helps to **identify and classify sensitive data**, which can then be subject to sector-specific and sector-neutral regulatory requirements under commercial law. Their enforcement, and violative considerations either could be subject to the provisions of the Digital Personal Data Protection Act, 2023 and the Code of Civil Procedure, 1908, and in certain aspects, even extended on questions of legitimate use under the DPDPA, and public law.

Inference

A potential AI Regulation could be helpful in the following contexts:

- *The regulation could require AI developers to disclose the types of data that their systems use and how that data is anonymized.*
- *The regulation* could also require AI developers to conduct impact assessments to identify the potential risks posed by their systems, including the risks of de-anonymization and discrimination, to enable technology-neutrality. This strengthens the use cases and test cases offered by AI companies, in terms of their economic and functional purposes, and enables a reasonably compliant AI ecosystem.
- In addition, the regulation could establish a certification process for AI systems, which is distinctive from how it is enabled through a National Data Management Office.

Issue Guidelines for Disclosure Norms

Provide guidance on how organizations can disclose data in a responsible and ethical manner, while also protecting privacy and security.

There will be certain tangible considerations which the Government must be mindful about, as they issue such guidelines:

- Sector-specific considerations
- Sector-neutral considerations
- Legal field-specific considerations
- Technology regulations under civil law and public law

Inference

- Develop guidelines for disclosure norms with respect to artificial intelligence systems that are specific to different types of data and different industries.

Draft Guidelines for the Creation of Searchable Data Inventories at the Ministries / Departments Levels

Makes easier for researchers and businesses to find and access the data they need to develop AI applications.

Inference

Since, the Government proposes the need to have a *Whole-of-Government Response* (like in the case of the Digital India Act proposal), it is necessary that open access inventories are created & maintained in cooperation with ministries and departments.

In addition, the Government has to enable and develop workable management guidelines which complement and strengthen the use of these inventories, and maintains inter-ministerial and inter-department cooperation at the level of nodal and subordinate authorities.

In the case of artificial intelligence, it would be required to develop separate inventory guidelines, considering the following scenarios:

- The interoperable use of inventory data and algorithmic infrastructure offered from the inventory of AI test cases and use cases
- The standalone use of AI test cases and use cases
- The ecosystem-related use of AI test cases and use cases in the government and business sectors

Issuance of Data Access & Licensing Agreements	Provides a framework for organizations to access and use government data in a legal and compliant manner.

Inference

Develop data access and licensing agreements that are fair and transparent, and that promote the use of data for innovation.

In addition, relevant licensing and access agreements with respect to the use of artificial intelligence would also have to be issued, either by the National Data Management Office, or any relevant authority, which are listed as follows:

- **AI software license agreement** *that grants the licensee the right to use AI software*
- **AI service level agreement (SLA)** *between a service provider and a customer required to define the level of service provided, which is categorised as an "AI Service"*
- **AI end-user license agreement (EULA) or AI end-client license agreement (ECLA)** *between a software vendor and an end-user or a client respectively to legitimise and mutually agree on the control and use of AI software*
- **AI explainability agreement** between software vendors and clients or customers requiring the company (vendor) to provide & submit explanations for the outputs of AI systems

Publication of Data Anonymization Guidelines	Helpful to ensure data anonymization to protect the privacy of individuals.

Inference

The NDMO would require to develop data anonymization guidelines that are aligned with international best practices and take into account the unique needs of Indian MSMEs and start-ups.

In the context of artificial intelligence systems, the following considerations are described in the context of data anonymization guidelines:

- In this context, a **technology-neutral** AI regulation could be helpful since the intent of such a proposed regulation could be to focus on the functional or economic characteristics of AI systems, rather than on the specific technologies that are used to develop or deploy them.
- **The principle of technology neutrality, in the case of data anonymization and even overall, must be implemented through such an AI regulation, regardless of the political, social, cultural, economic and logistic features of the AI systems subject to regulation.**
- This would allow the regulation to be more effective in protecting individuals from the risks posed by AI systems, even as technologies evolve. The regulation could require AI developers to conduct impact assessments to identify the potential risks posed by their systems, including the risks of de-anonymization.
- The regulation could require AI developers to implement appropriate mitigation measures to address the identified risks related to data anonymization protocols and measures.

Publish standards & principles for Fair and Ethical Use of Data	Provides guidance use of data in a responsible and ethical manner, to respect the rights of individuals.

Inference

The standards and principles on the fair and ethical use of data also inspire the need to have an AI regulation, because of the following reasons:

- While many or most standards and principles to ethicise the fair and ethical use of data have a direct impact in shaping artificial intelligence ethics standards & principles, the **degree of sophistication** required to shape those AI ethics standards would vary due to various factors.
- Those factors include:
  - Sector-specific impact of data protection ethics standards and principles, across jurisdictions
  - Corporate Governance and Knowledge Management Issues on the (1) Know-Hows and Know-Whys of AI systems and (2) Decisional hierarchies
  - Intellectual Property Models either designated by the Centres for Excellence or worked upon among companies otherwise
- Beyond the role of data protection ethics standards and principles, there are distinctive legal and policy issues related to the use and proliferation of artificial intelligence systems at multiple levels of engagement, development and production, which must be addressed differently, to avoid an unintended or unreasonable interplay of data protection and artificial intelligence ethics standards, in the spirit of promoting AI innovation in a New India.

#3 - Qualification Packs (QPs) and National Occupational Standards (NOS) for AI & Big Data

The second aspect, which infers the need to have a decent AI Regulation in India, is the reference to Qualification Packs (QPs) and National Occupational Standards (NOS) in the fields of artificial intelligence & big data. Based on the standards of the National Skill Development Corporation, the reference to **Levels 6, 7 & 8 QPs and NOS** in *the IndiaAI Expert Group Report, 1st Edition (2023)* has been provided.

Please note, that the inferences to have an AI Regulation are explained of the Qualification Packs and National Occupational Standards, based on **some of the AI Best Practices**, as referred to in the report.

Level 7

AI Best Practice	Inference
Applying a variety of pre-designed algorithmic models to specified use cases for internal and external clients.	An AI regulation could require AI developers to **conduct impact assessments** to **identify the potential risks posed by their models**, and to **implement appropriate mitigation measures**.
Evaluating the risks in deploying algorithmic models and developing mitigation measures for internal and external clients.	An AI regulation could require AI developers to **disclose the types of data that their AI models use** and **how that data is anonymized**, and to establish processes for auditing and monitoring the performance of their models.

Evaluating the performance of deployed algorithmic models at meeting expected business outcomes	An AI regulation could require AI developers to establish **quality assurance standards** for their models on a **sector-specific** and **technology-neutral basis**, and to provide transparency about the performance of their models to users.
Identifying the requirements of internal and external clients.	An AI regulation could require AI developers to **engage with users throughout the development and deployment process** to understand their needs and concerns.
Developing integrations for ensuring data availability for analytical or operational uses	An AI regulation could require AI developers to **document the data requirements of their models** and to provide clear guidance on how users can access and share data with their models, thereby **encouraging AI explainability**.
Defining data utilization and governance processes for the team or organization	An AI regulation could require AI developers to establish AI governance policies and procedures, and to train their employees on these policies and procedures, including those on **decisional & ethical hierarchies**. This could be helpful to maintain and encourage sustainable **AI-related knowledge management practices**.

Measuring the technical performance of algorithmic models for deployment.

An AI regulation could require AI developers to **conduct performance testing (taking into reference of the risk-based or impact-based use of AI)** of their models before deployment.

Inferences from Global-level AI Regulations

In this section, for a clear reference, we have examined and proposed the need to have an Artificial Intelligence Development & Regulation Bill based on regulatory developments in certain countries and a few key developments at an international level.

Chinese Regulations

Regulation / Draft Law	Features and Inference
Provisions on Regulating and Promoting Cross-border Data Flows *(Draft)*	The Chinese Government has a strict model of ownership within their own understanding of public interest over data belonging to Chinese citizens and entities, and the algorithms trained on such data processed. This draft law requires the conclusion of a personal information export contract, which is a form of **micromanaged contract enforcement practice** for the government. In the context of cross-border data flows, keeping the issue of cross-border data flow subject to **individual-to-entity contractual arrangements** and not established regulations or systemization gives the Chinese government an advantage to enforce such contracts rigorously with a microeconomic and trade law angle. This also reflects China's intent not to keep cross-border data flow a technocratic requirement.
Measures for the Management of Generative Artificial	The title is interesting to classify generative AI as a class of service. This is further affirmed in the Article 4 of the Measures.

Intelligence Services

Articles 5-7 of the Measures establish a hardcore approach of purpose of generative AI applications, based on the following features or needs of generative AI services:

- Optimization of use cases to enable a 'healthy' application ecosystem
- Independent innovation in basic generative AI solutions
- Strengthening of public data resource platforms for generative AI
- Increasing efficiency in use of computing resources
- Orderly opening of public data by type and grade and developing high-quality training data and resources

Article 8 makes it clear that providers must have **clear, specific and feasible tagging rules** (which mandatorily meet the requirement of these Measures). These tagging rules would be applicable in the case of **processed data, AI-generated content, and the personnel involved in enabling the generative AI services** respectively.

The Measures are clear that service agreements have to be signed to provide generative AI services.

Article 10 clearly explains China's intent not to let companies manufacture the consent of their users using generative AI services. The provision states that companies have to guide a user's scientific understanding of the AI tools. **Article 11** even goes further and makes it mandatory for companies to **not retain user input information and usage records, in an illegal manner**. This is significant in multiple aspects.

Article 14 focuses on the role of corporate governance & knowledge management in shaping the quality and efficiency of generative AI services offered. Companies are required under this provision to report to relevant departments about the quality of the training models of their AI system, and conduct measures such as model optimization training, and controlling transmission of the generative AI tools.

Like the "Provisions on the Management of Algorithmic Recommendations in Internet Information", this law also recognizes the concept of **public opinion properties**, which is a spatial and technocratic approach to regulate user opinion available in public as digital properties, with a restrictive approach.

Provisions on the Management of Algorithmic Recommendations in Internet

This is perhaps a regulation by China, which has a **straightforward approach** to recognize recommendation mediums, and recommendation algorithms in the context of internet. The purpose of defining recommendation algorithms as "**algorithmic**

Information Services

recommendation technology" seems to be direct and clear. However, the approach is maximalist while being specific. From a bureaucratic perspective, the provisions are airtight in an administrative sense. In addition, providing recommendation algorithms is categorized as a class of **service**.

Unlike other governments, recommendation algorithms (and therefore recommendation mediums) would be subject to coordinated means of governance under China's local internet information departments. This is again a **micromanaged** and **microeconomic** perspective to regulate recommendation algorithms.

Article 4 mandates that recommendation algorithms must respect **social mores**, showing the government's understanding of the impact of recommendation algorithms on the **socio-economic consciousness of digital users in China**, and how information overload could be caused by recommendation algorithms, for political and non-political reasons.

Article 7 establishes a comprehensive corporate governance ethics framework to govern the development, maintenance and democratization of algorithmic recommendation services, on the basis of the following steps:

- Implement entity responsibility for algorithm security

- Establish and complete management systems and technical measures, including:

  - Checking algorithm mechanisms
  - Technology ethics reviews
  - User registration
  - Checking published information
  - Data security
  - Personal information protections
  - Countering telecommunication network fraud
  - Security assessments and monitoring
  - Emergency response and handling of security incidents

- Draft and disclose the rules for algorithmic recommendation services

- Allocate professional staff and technical support corresponding to the scale of algorithmic recommendation services

Article 12 gives explicit measures to service providers of recommendation algorithms, such as:

- Utilize strategies for eliminating duplicate content

- Implement strategies to address fragmentation and intervention

- Optimize the transparency and explainability of rules for:
    - Searches
    - Sorting
    - Selections
    - Pushing
    - Displays
- Aim to avoid producing negative impacts on users
- Work towards preventing and reducing contention and disputes

Article 23 makes it explicit that an internet information department needs to establish a **hierarchical and categorical management system** perform the following functions:

- Conduct management by grade and category of algorithmic recommendation service providers
- Consider the public sentiment attributes and capacity to mobilize the public
- Take into account the content types provided by the algorithmic recommendation services
- Evaluate the scale of users served by the service providers
- Assess the importance of the data handled by the algorithmic recommendation technology

	• Consider the degree of interference in user conduct and other relevant factors
Provisions on the Administration of Deep Synthesis Internet Information Services	In this regulation, the services to offer deep fake technology are classified as a "deep synthesis internet information services", which makes sense. The provisions require deep synthesis service providers to: • Register with the CAC and obtain a license before operating • Implement measures to prevent the use of deep synthesis technology to create or disseminate illegal or harmful content • Label all deep synthesis content as such • Provide users with the ability to report deep synthesis content that they believe is illegal or harmful

A general assessment of all these regulations on artificial intelligence as per Chinese law, show the following traits:

- Their legal and administrative prerequisites are much maximalist in nature.
- The Chinese Government seems to have adopted and cultivated an administrative & regulatory approach towards both **data and algorithms** offered as a class of service, which could be defined as **hierarchical, customary and micromanaged**. This is reflective of the legalist, socialist and Confucian culture of Chinese legal scholarship. Colloquially, it is an **airtight approach**, which shows a trend of **effective ownership** over **data and algorithms** used in Chinese jurisdiction, by virtue of hierarchies of compliance under Chinese law.

- The Chinese Government treats public opinions **proprietary** in its definitive sense under public law, which means they consider the presence and flow of any public opinion within the jurisdiction of China, to be subject to reference-based **spatial control** and regulation by default.
- The compliance and administrative measures on artificial intelligence are less sophisticated and much more maximalist by nature.

For a potential AI Regulation in India, the following inferences could be made from Chinese regulations:

- The *IndiaAI Expert Group Report, 1st Edition (2023)* already proposes the structure and goals of a potential National Data Management Office (NDMO). Therefore, the AI Regulation must have 4 pillars of governance:
  - A **Whole-of-Government Approach to administrative law** (which includes digital public infrastructure and digital goods & services) in a **simplified** and **flexible** manner.
  - A **micromanaged approach** to regulate artificial intelligence technologies.
  - A **technology-aware** and **sector-specific approach** to classify artificial intelligence products, services and systems.
  - A **specific** and **transparent approach** to **regulate**, **recognize** and **certify proprietary** and **open-source** artificial intelligence **products, services and systems**.
- The approach to recognize the use cases of artificial intelligence does not have to be maximalist.

United States Regulations

Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

The Biden Administration recognizes the need to ensure **robust, reliable, repeatable, and standardized evaluations** of AI systems, which is clarified in the initial statements of the Executive Order.

The testing and evaluations of AI systems will also include **post-deployment performance monitoring**, which could be argued as a required compliance approach, for AI companies.

Another important requirement mentioned in the Executive Order is to develop **effective labeling and content provenance mechanisms** to track and flag AI-generated content.

The definition of artificial intelligence provided here, is flexible, and simplified, as opposed to the Annex 1 of the European Union's Artificial Intelligence Act. The reference to keywords such as "automation" and "model reference" give a technology-conscious approach to understand a simplified and basic analogy to recognize AI systems, within a legal framework.

The inclusion of **Infrastructure as a Service (IaaS) Product** in the Section 3 of this Executive Order, subject to the provisions of the *Section 5 of the Executive Order 13984 (2021)*, is quite interesting, in the case of artificial intelligence technologies. The definition in 2021 Executive Order was referenced in the context of **malicious cyber-enabled activities**.

Sections 3(ee), 3(ff) & 3(gg), which define "synthetic content", "testbed" and "watermarking" respectively, are important definitions in the context of AI systems. For example, the reference to **watermarking** as a principled definition signifies the

Executive Order's imperative to ensure that companies do conduct watermarking measures to detect how any AI-generated content, is authenticated to be AI-generated.

The Secretary of Commerce is required to propose regulations to require **US IaaS providers** (related to artificial intelligence infrastructure) to submit reports to the Secretary of Commerce when foreign persons use their compute infrastructure to train their AI models, and whether they could involve in a malicious cyber-enabled activity.

In the case of regulating the use of AI in biological sequencing, the Executive Order makes it clear that the Director of the OSTP has to

- Establish criteria and mechanisms for ongoing identification of biological sequences.
- Determine standardized methodologies and tools for conducting and verifying the performance of sequence synthesis procurement screening.
- Develop customer screening approaches to support due diligence in managing security risks posed by purchasers of biological sequences identified in **subsection 4.4(b)(i)(A)** of **Section 4**.
- Define processes for the reporting of concerning activity to enforcement entities.

It is indeed appreciative that specific regulatory requirements for scientific use cases, especially in domains like drug discovery and biological sequencing have been stated in the Executive Order, responsibly.

Section 4.2 of the Executive Order gives the Department of Commerce the power to require entities that are developing or planning to develop artificial intelligence (AI) models that could be used for both good and bad purposes (dual-use models) to provide regular reports on:

- Their development activities, including the security measures they are taking
- Who owns and has access to the model weights and how they are being secured
- The results of any safety tests they have run on the models

The Department of Commerce must also create rules that require foreign people who do business with Infrastructure as a Service Providers (IaaS) or their resellers to provide information about themselves and their transactions. At a minimum, these rules must require IaaS providers to:

- Verify the identity of the foreign person
- Keep records about the foreign person
- Report certain transactions

On content provenance and labelling, the Executive Order in **Section 4.5,** issues the requirement to develop science-backed guidelines, based on the following policy requirements:

(i) authenticating content and tracking its provenance;

(ii) labeling synthetic content, such as using watermarking;

(iii) detecting synthetic content;

(iv) preventing generative AI from producing child sexual abuse material or producing non-consensual intimate imagery of real individuals (to include intimate digital depictions of the body or body parts of an identifiable individual);

(v) testing software used for the above purposes; and

(vi) auditing and maintaining synthetic content.

These are simple, flexible and specific policy requirements for a potential regulation on AI-generated content.

In **Section *5.2***, the following actions are outlined to tackle concerns regarding intellectual property rights within the realm of AI:

- The Executive Order mandates the US Patent and Trademark Office to release guidance on patent eligibility concerning inventorship and the application of AI, encompassing generative AI.

- The Copyright Office will participate in providing suggestions for potential executive measures concerning copyright and AI. This includes aspects like the extent of protection for AI creations and the handling of copyrighted content in AI training.

Section *5.3* of the Executive Order has some fascinating provisions on artificial intelligence and competition law. As per the Section, the head of each US agency developing AI-related policies and regulations are required to

- Promote competition in AI and related technologies and other markets by **addressing risks from concentrated**

control, preventing unlawful collusion, and providing opportunities for small businesses and entrepreneurs.

- Encourage the Federal Trade Commission to consider the use of its existing authorities, including **rulemaking**, to **ensure fair competition in the AI marketplace** and protect consumers and workers from potential AI-enabled harms.
- Include competition-increasing measures in funding availability notices for commercial research-and-development facilities focused on semiconductors.
- Maximizing access to facility capacity for start-ups and small firms developing semiconductors for AI technologies.

Section 11(b)(i) of the Executive Order makes it clear that the Secretary of Commerce is required to establish a plan for global engagement on promoting and developing AI standards, which include:

(A) AI nomenclature and terminology;

(B) best practices regarding data capture, processing, protection, privacy, confidentiality, handling, and analysis;

(C) trustworthiness, verification, and assurance of AI systems; and

(D) **AI risk management**;

For a potential AI Regulation in India, the following inferences could be made from the Executive Order:

- The *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* of October 30, 2023 (United States), is a decent executive order with a sophisticated yet practical and tangible approach. The goals and essential points of focus of AI Regulation in the

Executive Order seem to be contextual in purpose and has some tangible legal definitions and principles on regulating and governing AI applications. The concept of Infrastructure as a Service Product is one such example.

- The Executive Order is keen to promote and develop effective product-service classifications of AI and related terminologies and nomenclatures for research and commercial purposes.
- The Executive Order recognizes the need for content provenance and watermarking of AI-generated content as a high priority.
- The Executive Order gives reasonable priority to legal issues surrounding patent eligibility concerning inventorship and the application of AI (including generative AI) and copyright protections.

European Union Regulations

The Artificial Intelligence Act

This is a pan-European regulation on the use and regulation of artificial intelligence systems, which was agreed by the member-states of the European Union, within the bounds of the Treaty of the Functioning of the European Union. The rationale behind the Artificial Intelligence Act comes from this understanding that AI's nature, often relying on extensive datasets and found in various products or services within the *European common market*, which means that this proposal's goals can't be accomplished by individual EU member-states. Moreover, varying national rules emerging in a patchwork fashion obstruct the smooth movement of AI-related products and services across the EU, making it less effective in safeguarding fundamental rights and Union values in different EU member-states. This aspect of subsidiarity is a crucial basis of the Artificial Intelligence Act.

As per the final document of the Artificial Intelligence Act, four policy options with different degrees of regulatory intervention were examined by the European Commission and the European Parliament.

- **Option 1**: *EU legislative instrument setting up a voluntary labelling scheme*;
- **Option 2**: *a sectoral, "ad-hoc" approach;*
- **Option 3**: *Horizontal EU legislative instrument following a proportionate risk based approach*;
- **Option 3+**: *Horizontal EU legislative instrument following a proportionate risk based approach + codes of conduct for non-high-risk AI systems*;
- **Option 4**: *Horizontal EU legislative instrument establishing mandatory requirements for all AI systems, irrespective of the risk they pose.*

The European Commission had adopted **Option 3+**, which in a larger aspect makes sense – since a horizontal hierarchy to regulate artificial intelligence technologies, with a risk-based approach has to be proportionate, which is where Option 4 does not seem feasible, and could affect the course of AI innovation.

Here are the key features of this legal instrument:

- The regulation classifies artificial intelligence into multiple **risk-based levels** (*(i) an unacceptable risk, (ii) a high risk, and (iii) low or minimal risk*).
- High-risk AI systems are subject to stricter regulatory requirements under this act, which are of two kinds as per the **Title III** of the Artificial Intelligence Act:
    - the AI system is **intended** to be used as **a safety component of a product**, or **is itself a product**, (covered by the Union harmonisation legislation listed in Annex II);

  - the product **whose safety component is the AI system**, **or the AI system itself** as a product, is **required to undergo a third-party conformity assessment** with a view to the **placing on the market** or **putting into service** of that product (pursuant to the Union harmonisation legislation listed in Annex II).
- The definition of artificial intelligence is expanded in the Annex I.
- For low or minimal risk AI systems, the Commission has preferred the **criteria** to designate such AI systems with risks (which means (1) risks of harm to the health or (2) risks of adverse impact to the fundamental rights, which is) equivalent or greater than the risks posed by high-risk AI systems. The criteria are described as follows:
  - *The AI system's intended purpose.*
  - *How much the AI system has been or will be used.*
  - *If the AI system caused harm, had an adverse impact on fundamental rights, or raised significant concerns. This should be based on reports or documented allegations submitted to national authorities.*
  - *The potential harm or adverse impact, including how severe it is and how many people it affects.*
  - *Whether people can opt out of the AI system's outcomes, and if not, why.*
  - *Whether people using the AI system are vulnerable due to power imbalances, knowledge gaps, economic disparities, social situations, or age.*
  - *If the AI system's outcomes can be easily reversed (note: health and safety impacts are not considered easily reversible).*
  - *Whether current EU laws offer effective ways to address AI system risks, excluding claims for damages.*
- It is required to establish risk management systems for high-risk AI systems, whose testing procedures will be based on **preliminarily defined metrics** and **probabilistic**

thresholds appropriate to the **intended purpose** of the high-risk AI system.

- The coverage of data governance in the context of AI systems in **Article 10** is also significant. Here is a list of the data governance and management practices, which are important to perform the **training, validation and testing of data sets**:
  - *the relevant design choices;*
  - *data collection;*
  - *relevant data preparation processing operations, such as annotation, labelling, cleaning, enrichment and aggregation;*
  - *the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent;*
  - *a prior assessment of the availability, quantity and suitability of the data sets that are needed;*
  - *examination in view of possible biases;*
  - *the identification of any possible data gaps or shortcoming and how these gaps and shortcomings are addressed.*
- The training, validation and testing of data sets must be performed (subject to the **intended purpose** of an AI system) in line with the characteristics or elements particular to the **geographical / behavioural / functional setting** of a high-risk AI system.
- **Article 14** defines the role of human oversight in overseeing high-risk AI systems through appropriate human-interface tools to minimize the *risks of health* or *adverse impact to fundamental rights*, subject to the intended purpose of a reasonably foreseeable misuse of the high-risk AI system.
- **Article 17** formulates the structure of a quality risk assessment for companies that are developing high-risk AI systems.
  - A plan for following regulations, including conformity assessments and managing changes to high-risk AI systems.

- Methods, procedures, and systematic steps for designing, controlling, and verifying high-risk AI systems.
- Methods, procedures, and systematic steps for developing, ensuring quality, and quality assurance of high-risk AI systems.
- Procedures for examining, testing, and validating high-risk AI systems before, during, and after development, along with how often these checks need to happen.
- **Technical specifications**, including standards, to be used, and a plan for making sure the high-risk AI system complies with the requirements in Chapter 2.
- Systems and procedures for managing data, from collecting and analysing to storing, filtering, mining, aggregating, and retaining data. These steps happen before and for the purpose of selling or using high-risk AI systems.
- A risk management system.
- Creating, implementing, and maintaining a **post-market monitoring system**, as described in Article 61.
- Procedures for reporting serious incidents and malfunctions.
- How to communicate with national authorities, other operators, customers, and interested parties.
- Systems and procedures for keeping records of all relevant documents and information.
- Managing resources, including measures related to **supply security**.
- An accountability framework detailing the responsibilities of management and staff concerning all the aspects listed above.

- Any third party (for example, a distributor, importer etc.,) shall be considered as a provider, if they are anyways making a **substantial modification** to the high-risk AI system or they **modify the intended purpose** of the high-risk AI

system or **put it into the market or offer the high-risk AI system as a service** under their name or trademark.

The inferences from the Artificial Intelligence Act, for India's potential AI regulation are described as follows:

- India should adopt a risk-based approach to regulate artificial intelligence, which has context-specific and strategic-sector-specific considerations involved.
- Defining if an AI system's risk is subject to examination considering their intended purpose or their reasonably foreseeable misuse, is an interesting policy choice to be made.
- India's potential AI regulation must have quality assessment and risk assessment frameworks for AI systems. At least for quality assessment, the coverage could expand to AI systems with low or minimal risks, and of those in the strategic and government sectors.

The Bletchley Declaration in the AI Safety Summit, 2023

The Bletchley Declaration agreed upon by several countries including India focuses on a prima facie arrangement to recognize AI risks and how AI safety measures could be legalized at multilateral and domestic levels.

- The Declaration's initial statements focus on safety risks related to **highly capable general-purpose AI models** in domains such as **cybersecurity and biotechnology**. Such huighly capable general-purpose AI models include **foundational models** capable to perform variety of tasks, and specific **narrow AI** applications with exceeding capabilities and the potential to cause harm.
- According to the Declaration, AI-related risks can stem from **intentional misuse** or **unintended control problems related to aligning with human intent**.

- The Declaration suggests that countries may **classify and categorize risks based on their national context and legal frameworks when appropriate**.
- The Declaration has rightly pointed out that many risks arising out of artificial intelligence technologies are inherently **international** (or globalized) in nature.
- The Declaration emphasizes to prioritise **safety throughout the entire AI development process**. However, developers of **cutting-edge AI technologies** (referred as *Frontier AI* in the Declaration), particularly those with **exceptional power and potential for harm**, bear a special responsibility for ensuring the safety of their creations. This entails implementing **safety testing procedures,** conducting thorough evaluations, and employing other suitable safeguards.
- The Declaration offers an appeal to all relevant stakeholders to provide **transparent** and **accountable explanations** of **their strategies** for **assessing, monitoring, and mitigating potential risks** and adverse consequences associated with their AI systems. This is particularly crucial for preventing misuse, control issues, and the exacerbation of other hazards.
- The **key agenda** of the parties to this Declaration is described in the following points:
  - Emphasize the importance of identifying **shared AI safety risks** and **maintaining a collective understanding** as AI capabilities advance globally.
  - Highlight the need for **risk-based policies** in individual countries to ensure safety.
  - Promote **collaboration** among nations while acknowledging that approaches may vary based on **national context and legal systems**.
  - Stress the importance of **transparency** by private entities developing **advanced AI technologies**.

- Suggest the development of **evaluation metrics, safety testing tools, and the enhancement of public sector capabilities** and scientific research in this context.

The UNESCO Recommendation on the Ethics of Artificial Intelligence (2021)

We reiterate the **positions** of the Indian National Commission for Cooperation with UNESCO on the UNESCO Recommendation on the Ethics of Artificial Intelligence, and recommend that the position within the bound of the Commission's submissions may be incorporated in India's potential AI Regulation. The ten principles, four values, and ten policy intervention areas by the Commission are described as follows:

- *To recognize that through the* **right to development**, *all fundamental freedoms and human rights can be realized fully and the full enjoyment of AI technologies for all.*
- *Enhancement of scope from a domain perspective, not limiting it to* **mandated domains** *as prescribed by UNESCO and technological perspective, extends the range from merely AI-human interaction and covers emerging technology like IoT, ML, Deep Learning, etc.*
- *To include* **AI Readiness, EIA of AI-based techs, Assessment of AI for all stakeholders, and effectiveness and efficiency of policies for AI Ethics in Checklist Matrix**.
- *Three suggestions in Policy areas 3, 4, and 5 – for Ethical Governance, a checklist on explainability and transparency requirements must be implemented internationally. For Development and International Cooperation,* **access to the dataset is suggested to maintain commensurate value realization and dataset provider**. *Finally, a checklist matrix*

that is **globally accepted for ecosystem and environment** *must be worked out for ecosystem and environment.*

- *In addition to accountability,* **transparency, responsibility, efficiency, effectiveness, algorithms, datasets, affordable AI solutions, and devices** *must also be considered part of the principles because there is a* **potential risk of creating digital and AI have-nots**.
- *Equitable access to hardware for design and development of AI solution and AI-enabled device for weaker section of the society.*
- *Access to AI solutions in local languages to bridge the language divide in countries like India, with more than twenty constitutionally recognized languages.*
- **A global treaty that would ensure to avoid any harmful use of emerging technology in subversion activities using AI by member-states as well as non-state actors across the transnational borders.**
- **AI and Data Sovereignty**, *in a manner that strengthens State's sovereignty, at the same time it does not affect the State in making the choices of* **governance, legislation, and development models in the AI environment**.

The Hiroshima AI Process Comprehensive Policy Framework (G7)

Here are the inferences from the Hiroshima AI Process Comprehensive Policy Framework:

- **Mandate Risk Management**: Establish a mandatory requirement for AI developers to implement comprehensive risk management frameworks throughout the AI lifecycle, subject to sector-specific, sector-neutral and strategic sector-related requirements.

- **Promote Traceability and Documentation**: Encourage developers to maintain traceable records of datasets, processes, and decisions made during AI development.

- **Address Specific Risks**: Specifically address the identified risks, such as:

    - CBRN risks,
    - offensive cyber capabilities,
    - health and safety risks,
    - self-replication,
    - societal risks, and
    - **systemic risks**.

- **Post-Deployment Monitoring**: AI developers should continuously monitor their deployed systems to identify and address vulnerabilities, incidents, and patterns of misuse.
- **Third-Party Vulnerability Reporting**: Encourage third-party and user involvement in vulnerability discovery and reporting through mechanisms like bounty programs or contests.
- **Incident Reporting and Mitigation**: Maintain appropriate documentation of reported incidents and collaborate with stakeholders to mitigate identified risks and vulnerabilities.
- **Responsible Information Sharing**: Establish mechanisms for organizations to share relevant information, including evaluation reports, security and safety risk assessments, and information about potential misuse or circumvention of safeguards.
- **Shared Standards and Best Practices**: Develop and adopt shared standards, tools, mechanisms, and best practices for ensuring the safety, security, and trustworthiness of advanced AI systems.

- **AI-Generated Content Identification**: Develop and implement mechanisms to enable users to identify AI-generated content, such as watermarks or other techniques.
- **Content Provenance**: Provide provenance data for AI-generated content, including the identifier of the AI system used.
- **Research Prioritization**: Prioritize research on mitigating societal, safety, and security risks associated with advanced AI systems.
- **Investment in Mitigation Tools**: Invest in developing and implementing appropriate mitigation tools to address AI-related risks.

Inferences based on Body of Research by Indic Pacific Legal Research and the Indian Society of Artificial Intelligence and Law

These are all the inferences from relevant government documents, developments in the international AI governance landscape and the body of research developed by Indic Pacific Legal Research & the Indian Society of Artificial Intelligence and Law.

Regularizing Artificial Intelligence Ethics in the Indo-Pacific, GLA-TR-002 (2021)

Multilateralism and Plurilateralism

- Consider a multilateral approach to AI ethics negotiations and design.
- Acknowledge the potential challenges of implementing top-down multilateral approaches.
- Explore plurilateral approaches to address regulatory competence and leverage concerns.

Indigenization, Localization, and Economic Rights (ILER)

- Integrate ILER principles into AI development and deployment in the Indo-Pacific region.
- Adopt a step-by-step approach to align AI capabilities with regional and local needs.
- Develop regional and local consensuses on AI applications and policies.

- Utilize the SOTP Classification (Subject, Object, Third Party) to assess economic impacts and foster cooperation.

Human-Centric Approach (HCA) and Rights-based Approach (RiCA)

- Adopt a human-centric approach to AI that is not unrealistic or in conflict with agreed-upon RCAs (Risk-centric Approaches).

- Avoid limiting the scope of review and decision-making to a purely rights-based approach.

- Understand the centrality of human beings by addressing the risks of algorithmic anthropomorphism.

- Prioritize RiCAs that are relevant to strategic and risk considerations.

- Consider the following approaches to integrating RiCAs, RCAs, and HCAs:

    - RiCAs can inform HCAs, which in turn shape RiCAs.

    - HCAs can be based on RCAs, which then influence RiCAs.

    - RCAs can focus on algorithmic anthropomorphism, a core component of HCAs, which can shape RiCAs.

Addressing Risks in Specific Fields

- Develop HCAs to address emerging risks in fields such as environmental sciences, cybersecurity, telecommunications, commercial and economic law.

- Utilize HCAs to counter and understand algorithmic anthropomorphism in these fields.

- Leverage HCAs to inform the development of RiCAs and RCAs in these areas.

Convergence of RiCAs, RCAs, and HCAs

- Pursue convergence of RiCAs, RCAs, and HCAs to establish a comprehensive AI-related regulatory and foresight network.

- Align RiCAs to ensure a comprehensive AI-related rights-based regulatory framework.

- Expand the scope of alignment for RCAs.

- Optimize the anthropological element of HCAs to maximize risk realization.

- Implement effective feedback mechanisms to address enforcement challenges.

Indigenization, Localization, and Economic Rights (ILER) in Implementation

- Integrate ILER principles into the implementation of AI regulations.

- Consider regulatory competence and leverage concerns when implementing ILER principles.

- Address R&D, skill, manufacturing, and service sector compliance issues related to ILER.

- Effectively shape the optimal and larger quotient of risk (OLQR) through ILER implementation.

Regulatory Sandboxes for Artificial Intelligence: Techno-Legal Approaches for India, ISAIL-TR-002 (2022)

Shift from Sectoral to Technological Approach

- Transition from a sectoral approach to a technology-wise approach for regulatory sandboxes.
- Recognize the limitations of sectoral sandboxes and the need for a broader framework.
- Formulate a principal legislation for regulatory sandboxes instead of relying on delegated legislation.

Establishment of Statutory Innovation Offices

- Create a statutory Innovation Office at the Central level and State Innovation Offices along with statutory authorities.
- Define the roles, responsibilities, and powers of these Innovation Offices.
- Ensure coordination between Central and State Innovation Offices.

Mandatory Provisions and Flexibility for Specific Regulations

- Include mandatory provisions for definitions, duration, and exit criteria in the principal legislation.
- Allow for delegated legislation to address specific regulations, rules, guidelines, and frameworks for different technology combinations.

Eligibility and Entry Requirements

- Prescribe eligibility and entry requirements for participation in regulatory sandboxes through delegated legislation.
- Standardize the duration of regulatory sandboxes to 12 months (extendable for 6 months in exceptional cases).
- Mandate regular monitoring and reporting of progress for each cohort.

Incentives and Concessions

- Provide incentives such as relaxation of licensing requirements, concessions in electricity duties, and GST concessions for supplies during the sandbox period.
- Implement a Concession Agreement between the Innovation Office and the innovator company to ensure proper utilization of incentives.

Consumer Protection and Dispute Resolution

- Mandate minimum insurance requirements for innovator companies.
- Require innovator companies to obtain consent from consumers participating in the sandbox framework.
- Implement a robust dispute resolution mechanism using a hybrid Med-Arb approach.
- Establish a panel of mediators and arbitrators with expertise in AI and technology law.

Interdepartmental Cooperation

- Enable Innovation Offices to actively undertake interdepartmental cooperation with Central Ministries, State Governments, and sectoral regulators.

Overall Harmonization and Robust Legal Framework

- Harmonize the regulatory framework for regulatory sandboxes across different sectors and technologies.
- Establish a robust legal framework to facilitate technological innovation.
- Promote the adoption of AI technologies in various sectors for overall economic growth and development.

Deciphering Artificial Intelligence Hype and its Legal-Economic Risks (VLiGTA-TR-001, 2022)

- **Transparency and Ethical Design:** Implement clear guidance for companies to inform regulators about their investments and ethical designs concerning AI products, especially those utilizing narrow AI and high-intensive AI technologies.
- **Knowledge Management Systems:** Emphasize the importance of efficient knowledge management systems that address intellectual property issues and consider economic and ethical implications linked to AI technologies.
- **Risk-Oriented Practices:** Encourage risk-oriented transparency regarding data protection, privacy, and algorithmic operations, especially for AI technologies integrated at various managerial levels.

- **Ethical Free Flow of Data:** Advocate for negotiating ethical data flow agreements between countries to manage AI-related hype and support public welfare in data exchange.
- **Consultative Framework:** Consider the proposed working conditions to determine AI hype as a reference framework to interlink competition policy and technology governance.
- **Model Algorithmic Ethics Standards (MAES):** Propose the use of Model Algorithmic Ethics Standards to initiate estimations and support regulatory sandboxes.

Deciphering Regulative Methods for Generative AI (VLiGTA-TR-002, 2023)

- **Regulations for Intellectual Property Rights:** Develop and enforce regulations to address ownership of generated content, secure original creations, and establish guidelines for licensing and usage in generative AI.
- **Data Security and Transparency:** Create strict safeguards for data security and privacy in generative AI, encouraging transparent and understandable AI models to ensure accountability and mitigate risks.
- **Industry Standards:** Utilize the developed ontological categories for industry classifications, and implement suggestions on Product-Service Classifications as discussed in Chapter 4.
- **Certification Procedures:** Establish standard testing and certification methods to ensure reliability, safety, and compliance of generative AI systems.
- **Global Inclusivity:** Acknowledge the concerns of Global South countries, including India, while formulating regulations to prevent industry standards that might not be applicable.

Recommendations on India's Digital Public Infrastructure

- **Local Generative AI Engine:** Advocate for the creation of a native generative AI engine for India's Digital Public Infrastructures (DPIs) to enhance technological independence, localization, data sovereignty, and economic opportunities.

Recommendations on India's Regulatory Infrastructure

- **Ethical Principles and Regulatory Sandboxes:** Establish ethical principles for generative AI and create controlled environments for innovators and developers to experiment with AI technologies, supported by effective regulatory frameworks.
- **AI-enabled Dispute Resolution:** Support the integration of AI in Online Dispute Resolution (ODR) platforms, ensuring it leads to effective and efficient dispute prevention and resolution.

Promoting Economy of Innovation through Explainable AI (VLiGTA-TR-003, 2023)

- **Converging Legal and Business Concerns:** Suggest using Explainable AI (XAI) to address legal and business concerns, focusing on regulatory challenges, risk management, and compliance.
- **Conflict Management and Innovation:** Recommend compliance by design to encourage innovative management, de-risking AI, and risk mitigation strategies through decentralized and transdisciplinary approaches.

These inferences highlight the importance of various aspects, including transparency, ethical design, data security, compliance by design, and the promotion of innovation while managing AI-related risks and regulatory challenges in India.

The Artificial Intelligence (Development & Regulation) Bill – Draft

Based on the inferences provided in the previous chapter, and the proposed **New Artificial Intelligence Strategy for India**, we propose the contents of the **Artificial Intelligence (Development & Regulation) Act**, in three parts – (1) legal substance; (2) governance provisions; (3) use-specific provisions.

The reason we have proposed the name of this proposed bill to be the **Artificial Intelligence (Development & Regulation) Bill**, is that having a pro-innovation and pro-development approach to regulate AI and develop AI ecosystem, must be clear legislative intent of this bill, within our constitutional framework.

The key ministry with whom this proposed law must be associated has to be the Ministry of Electronics and Information Technology, Government of India.

The contents of the bill are proposed to cover the following legal and policy aspects surrounding the use, development and regulation of AI technologies.

Definition of Artificial Intelligence

Artificial Intelligence (AI) an information system that uses computational, statistical, or machine-learning techniques to produce outputs from a given set of inputs. It is also a diverse class of technology encompassing various sub-categories of **technical**, **commercial**, and **sectoral** nature.

For the purposes of this bill, **artificial intelligence is further classified in technical and commercial aspects as a product, service or system**.

Another kind of classification offered for the purposes of this bill is the classification of **artificial intelligence as a concept**.

The conceptual classification of Artificial Intelligence to conduct ethical and legal evaluation of the use, development, maintenance, regulation and proliferation of artificial intelligence technologies is provided as follows:

- **Technical Concept Classification:** This approach estimates the legal and policy risks associated with technical use cases of AI systems at a conceptual level.
- **Issue-to-Issue Concept Classification:** AI systems are assessed on an issue-specific basis, determining their conceptual nature.
- **Ethics-Based Concept Classification:** AI is shaped as a concept by ethical theories, especially in matters concerning regulation and adjudication.
- **Phenomena-Based Concept Classification:** Beyond technical and ethical considerations, this classification addresses rights-based issues due to the use of AI systems, particularly concerning natural and human-related phenomena.
- **Anthropomorphism-Based Concept Classification:** This classification considers scenarios where AI systems conceptually anthropomorphize human attributes and realities through intervention. It involves re-evaluating the influence AI systems have for regulatory and adjudicatory purposes. This transformation challenges traditional views of the symbiotic relationship between AI and human environments, influencing human identity, languages, cultures, rights, systems, and societies.

Another method to classify the adjudicatory and legal standing of artificial intelligence technology, is to classify its status as a legal entity or a juristic entity. In that regard, **we propose that artificial intelligence must be recognized as a juridical person in the definitions of the bill**.

Coverage of the Draft Bill

The Bill covers the following areas:

- Stratification of artificial intelligence on a risk-basis for adjudicatory, regulatory and enforcement purposes into (1) narrow risk AI systems; (2) medium risk AI systems; (3) high risk AI systems and (4) unintended risk AI systems.
- Prohibition of unintended risk AI systems
- Sector-specific standards for high-risk AI systems with inherent purpose associated with strategic and non-strategic sectors, such as telecom, space, health, digital public infrastructure, energy, biotechnology, and others.
- A framework for the Quality Assessment and Risk & Vulnerability Assessment of high-risk AI systems
- Certification of artificial intelligence systems, and of the ethical, technical and commercial practices associated with the use, research & development and commercialization of AI systems.
- Ethics code for the development, procurement and commercialization of artificial intelligence technologies, with a pro-innovation, pro-development and technology-neutral approach of AI governance
- Model standards on practices of knowledge management and decision-making on the development, maintenance and compliance of artificial intelligence systems for companies irrespective of risks
- Constitution, functionalization and the intra-governmental operability of the **IndiaAI Development & Regulation**

Council (IDRC) as a statutory & regulatory body with a whole-of-government approach to coordinate across government bodies, ministries and departments.

- Guidance principles for relevant agreements related to the use, development and commercialization of artificial intelligence technologies.
- Post-deployment monitoring of high risk AI systems
- Third-party vulnerability reporting of risks associated with high risk AI systems
- Incident reporting and mitigation in the case of AI systems
- Responsible information sharing in the case of all AI systems
- Spatial-level standards & knowledge management practices for rendering intellectual property protections for artificial intelligence systems in laws of patent, copyright, trademarks and industrial design
- Shared sector-neutral standards and best practices in the case of all AI systems
- Standards of assessment of manipulative anti-competitive practices involving the use, research & development, production, marketing, democratisation and evaluation of artificial intelligence systems in the digital market
- Standards for the content provenance, identification & watermarking of AI-generated content
- Employment and skill security standards due to the associated risks posed by artificial intelligence systems
- Insurance policy for the research & development, production and implementation of artificial intelligence technologies
- Concurrent provisions related to legal frameworks including the Digital Personal Data Protection Act, 2023 and the proposed Digital India Act

A Draft National Data Management Office Act

We have stated the provisions of a draft National Data Management Office Act, based on the *IndiaAI Expert Group Report, 1st Edition (2023)*, for the purposes expanding certain provisions of the **Artificial Intelligence (Development & Regulation) Bill, 2023**.

Definitions

(a) "NDMO" stands for the National Data Management Office, established as a statutory body.

(b) "CEO" refers to the Chief Executive Officer of the NDMO, who heads and manages the affairs and operations of the NDMO.

(c) "Functional Divisions" denote the six functional divisions within the NDMO, including Standards and Policies Division, Platforms and IT Division, Grievance Redressal Division, Legal Division, Audit and Compliance Division, and HR & Finance Division.

(d) "Experts" signify individuals with expertise in relevant fields who may be assigned to specific functional divisions to provide technical and operational support.

(e) "Data Management Units (DMU)" represent institutional mechanisms established within each Ministry/Department to manage data-related affairs in accordance with the National Data Governance Policy (NDGP).

(f) "Data Fellows" are officers within the DMU, supported by the Ministry of Electronics and Information Technology (MeitY), responsible for carrying out specific data-related functions.

CHAPTER II: NATIONAL DATA MANAGEMENT OFFICE (NDMO)

Establishment of NDMO

(1) The National Data Management Office (NDMO) is hereby established as a statutory body for the governance, management, and regulation of data-related affairs in India.

(2) The NDMO shall be responsible for providing general direction on the management of data affairs and operations in line with the provisions of the National Data Governance Policy (NDGP).

Chief Executive Officer of NDMO

(1) The NDMO shall be headed by a Chief Executive Officer (CEO) who is responsible for the overall management of the NDMO's affairs and operations.

(2) The NDMO shall be responsible for providing general direction on the management of data affairs and operations in line with the provisions of the National Data Governance Policy (NDGP).

Functional Divisions of NDMO

(1) The CEO may be supported by heads of six functional divisions within the NDMO:

(a) Standards and Policies Division

(b) Platforms and IT Division

(c) Grievance Redressal Division

(d) Legal Division

(e) Audit and Compliance Division

(f) HR & Finance Division

(2) Experts from the project management unit may be assigned to relevant divisions to provide technical and operational support.

CHAPTER III: DATA MANAGEMENT UNITS (DMU)

Establishment of DMUs

(1) In accordance with the NDGP, Data Management Units (DMUs) may be established within each Ministry/Department to manage data-related affairs.

(2) The roles and responsibilities of the DMUs shall be to qualify the expected outcomes and standardize operations across all line ministries/departments.

Structure of DMU

(1) The structure of each DMU shall be created in accordance with the NDGP, detailing the functional and technical requirements of each division/officer within the DMU.

(2) Data Fellows, supported by the Ministry of Electronics and Information Technology (MeitY), shall carry out specific data-related functions within the DMU.

The Draft Bill

CHAPTER I: PRELIMINARY

Section 1 - Short Title and Commencement

(1) This Act may be called the **Artificial Intelligence (Development & Regulation) Bill, 2023**.

(2) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the coming into force of that provision.

Section 2 – Definitions

[Please note: we have not provided all definitions, which may be required in this bill. We have only provided those definitions which are more essential, in signifying the legislative intent of the bill.]

In this Bill, unless the context otherwise requires,—

(a) "Artificial Intelligence", "AI", "artificial intelligence application", "artificial intelligence system" and "AI systems" mean –
  (i) an information system that employs computational, statistical, or machine-learning techniques to generate outputs based on given inputs. It is a diverse class of technology encompassing various sub-categories of technical, commercial, and sectoral nature, on the basis of the means of classification provided as follows –
    a. Conceptual Classification: AI is conceptually classified for the ethical and legal evaluation of its use, development, maintenance, regulation, and

proliferation. This classification is further categorised as –

i. Technical Concept Classification means the process of estimating the legal and policy risks associated with technical use cases of AI systems at a conceptual level;
ii. Issue-to-Issue Concept Classification means the process of assessing AI systems on an issue-specific basis to determine their conceptual nature;
iii. Ethics-Based Concept Classification means the process of shaping AI as a concept based on ethical theories, particularly in matters concerning regulation and adjudication;
iv. Phenomena-Based Concept Classification means the process of addressing rights-based issues due to the use of AI systems, focusing on natural and human-related phenomena; and
v. Anthropomorphism-Based Concept Classification means the process of evaluating scenarios where AI systems conceptually anthropomorphize human attributes and realities, thereby challenging traditional views of the symbiotic relationship between AI and human environments.

b. Technical and Commercial Classification: AI is classified as a product, service, or system in its technical and commercial aspects.

(b) "AI-Generated Content" means content, physical or digital that has been created or significantly modified by an Artificial Intelligence (AI) system, which includes, but is not limited to, text, images, audio, and video created through a variety of techniques, subject to the test case or the use case of the artificial intelligence application;

(c) "Appellate Tribunal" means the Telecom Disputes Settlement and Appellate Tribunal established under section 14 of the Telecom Regulatory Authority of India Act, 1997;

(d) "Content Provenance" means the identification, tracking, and watermarking of AI-generated content to establish its origin and authenticity.

(e) "Data" means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means;

(f) "Data Fiduciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data;

(g) "Data Principal" means the individual to whom the personal data relates and where such individual is—

(i) a child, includes the parents or lawful guardian of such a child;

(ii) a person with disability, includes her lawful guardian, acting on her behalf;

(h) "Data Processor" means any person who processes personal data on behalf of a Data Fiduciary;

(i) "Data Protection Officer" means an individual appointed by the Significant Data Fiduciary under clause (a) of sub-section (2) of section 10 of the Digital Personal Data Protection Act, 2023;

(j) "Digital Office" means an office that adopts an online mechanism wherein the proceedings, from receipt of intimation or complaint or reference or directions or appeal, as the case may be, to the disposal thereof, are conducted in online or digital mode;

(k) "Digital personal data" means personal data in digital form;

(l) "Employment and Skill Security Standards" means regulations and practices addressing risks arising from the

deployment and utilization of artificial intelligence systems concerning employment and skills;

(m) "Ethics Code" means set of principles and guidelines governing the development, procurement, and commercialization of artificial intelligence technologies with an approach fostering innovation and technology-neutral AI governance;

(n) "High Risk AI Systems" means artificial intelligence systems with significant potential risks and are classified as high risk as per the risk-stratification framework outlined in this Bill;

(o) "IDRC" means IndiaAI Development & Regulation Council, a statutory and regulatory body established to oversee the development and regulation of artificial intelligence systems across government bodies, ministries, and departments;

(p) "Inherent Purpose" means the underlying objective or goal for which an artificial intelligence system is designed, developed, and deployed, and that it encompasses the specific tasks, functions, or capabilities that the artificial intelligence system is intended to perform or achieve;

(q) "Insurance Policy" means measures and requirements concerning insurance for research and development, production, and implementation of artificial intelligence technologies;

(r) "Juridical Person" means an artificial intelligence technology recognized as a juridical person under the definitions of this Bill;

(s) "Medium Risk AI Systems" means artificial intelligence systems with moderate potential risks, identified in the medium risk category within the risk-stratification framework set out in this Bill;

(t) "Narrow Risk AI Systems" means artificial intelligence systems assessed to have minimal potential risks and fall within the lowest risk stratum as per the risk-stratification framework provided in this Bill;

(u) "Person" includes—

(i) an individual;
(ii) a Hindu undivided family;
(iii) a company;
(iv) a firm;
(v) an association of persons or a body of individuals, whether incorporated or not;
(vi) the State; and
(vii) every artificial juristic person, not falling within any of the preceding sub-clauses including otherwise referred to in sub-section (p) of the Bill;

(v) "Post-Deployment Monitoring" means all activities carried out by the data fiduciaries or third-party providers of AI systems to collect and review experience gained from the use of the artificial intelligence systems they place on the market or put into service for the purpose of identification to reasonably foresee to apply any preventive or corrective actions;

(w) "Quality Assessment" means the evaluation and determination of the quality of AI systems, encompassing technical, ethical, and commercial aspects;

(x) "Risk & Vulnerability Assessment" means the comprehensive analysis of potential risks and vulnerabilities associated with AI systems, particularly high-risk AI systems;

(y) "Significant Data Fiduciary" means any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government under section 10 of the Digital Personal Data Protection Act, 2023;

(z) "State" means the State as defined under article 12 of the Constitution;

(aa) "training data" means data used for training an AI system through fitting its learnable parameters, which includes the weights of a neural network;

(bb) "Unintended Risk AI Systems" means AI systems that are prohibited under the provisions of this Bill due to their potential risks;

(cc) "testing data" means data used for providing an independent evaluation of the artificial intelligence system subject to training and validation to confirm the expected performance of that AI system before its placing on the market or putting into service;

(dd)"use case" means a specific application of an artificial intelligence system to solve a particular problem or achieve a desired outcome;

CHAPTER II: CATEGORIZATION AND PROHIBITION

Section 3 - Stratification of AI Systems

(1) AI systems shall be classified into four categories based on their inherent risk –

(a) Narrow risk AI systems: AI systems that pose a low level of risk to individuals, society, or the environment;

(b) Medium risk AI systems: AI systems that pose a moderate level of risk to individuals, society, or the environment;

(c) High risk AI systems: AI systems that pose a significant level of risk to individuals, society, or the environment; and

(d) Unintended risk AI systems: AI systems that are not deliberately designed or developed but emerge from the complex interactions of AI components and may pose unforeseen risks.

(2) All the AI systems designated in the categories above as per sub-section (1), except stated otherwise in the Section 5 (1) shall be examined on the basis of their inherent purpose, which is subject to the basis of the means of classifications provided in sub-section (a)(i) of Section 2 of the Bill, the listing of classes of

artificial intelligence systems in Schedule III and the following risks and vulnerabilities as examined:

(i) The extent to which the AI system has been utilized or is expected to be employed shall be considered by the IDRC;

(ii) The assessment shall include an examination of the potential harm or adverse impact, taking into account its severity and the number of individuals affected.

(iii) In case it does not remain feasible for data principals to have the ability to opt out of the AI system's outcomes, then the reasons for such limitations shall be examined by the IDRC;

(iv) The assessment shall consider the vulnerability of data principals using the AI system, taking into those foreseeable factors as may be prescribed which may limit the autonomy of the data principles to realise and foresee the vulnerability of using the AI system;

(v) It shall be determined whether the outcomes produced by the AI system can be easily reversed;

(3) If the use case of an AI system not prohibited under Section 4 is associated with strategic industry sectors referred to in Schedule II, then the set of risks & vulnerabilities required to be examined as per sub-section (2) shall have to be examined subject to the legitimate uses designated in the provisions of the Section 7 of the Digital Personal Data Protection Act, 2023 and otherwise as may be prescribed.

Section 4 - Prohibition of Unintended Risk AI Systems

The development, deployment, or use of unintended risk AI systems as listed in Schedule III is prohibited.

CHAPTER III: SECTOR-SPECIFIC STANDARDS FOR HIGH-RISK AI SYSTEMS

Section 5 - High-Risk AI Systems in Strategic Sectors

(1) Sector-specific standards shall be developed for high-risk AI systems in strategic industry sectors as designated by the Central Government in Schedule II.

(2) These standards shall address issues such as safety, security, *reliability*, *transparency*, *accountability*, and *ethical considerations* subject to the legitimate uses designated in the provisions of the Section 7 of the Digital Personal Data Protection Act, 2023 and otherwise as may be prescribed.

CHAPTER IV: CERTIFICATION AND ETHICS CODE

Section 6 - Certification of AI Systems

(1) A certification scheme for AI systems shall be established.

(2) This scheme shall certify AI systems that meet the requirements of this Bill and other applicable laws as referred to in Schedule I.

(3) The purpose of every certification scheme is to identify and examine the inherent purpose of an AI system based on their risk levels designated in Section 3, and the means of classification provided in sub-section (a)(i) of Section 2 of the Bill, and listed in Schedule III.

Section 7 - Ethics Code for Narrow & Medium Risk AI Systems

(1) An Ethics Code for the development, procurement, and commercialization of artificial intelligence technologies shall be established.

(2) This Ethics Code shall promote responsible AI development and utilization while addressing the potential risks associated with AI technologies.

(3) The Ethics Code shall be based on the following principles:

(a) AI systems shall respect human dignity and well-being;

(b) AI systems shall be fair and non-discriminatory;

(c) AI systems shall be transparent and explainable;

(d) AI systems shall be accountable;

(e) AI systems shall respect privacy and data protection as per the provisions of the Digital Personal Data Protection Act, 2023;

(f) AI systems shall be secure and safe;

CHAPTER V: KNOWLEDGE MANAGEMENT AND DECISION-MAKING

Section 8 - Model Standards on Knowledge Management

(1) The IRDC shall develop and prescribe comprehensive model standards on knowledge management and decision-making processes concerning the development, maintenance, and compliance of artificial intelligence systems for all companies operating within the jurisdiction of India, regardless of the assessed risk levels of their AI systems.

(2) These model standards shall encompass the following areas:

(a) Effective knowledge management practices and procedures to ensure the quality, reliability, and security of data used for training, validating, and improving AI systems.

(b) Model governance frameworks that define the roles and responsibilities of individuals, departments, or committees involved in AI model development, deployment, and monitoring.

(c) Transparent decision-making procedures, including the establishment of model selection criteria, model performance assessment, and ethical considerations in AI system operation.

(3) All entities, whether public or private, that are engaged in the development, deployment, or utilization of artificial intelligence systems shall be bound by the model standards on knowledge management and decision-making as provided by this section.

(4) Entities already operating AI systems within the jurisdiction of India shall comply with the prescribed model standards within a reasonable timeframe, as determined by the IRDC. The compliance timeline may vary based on the complexity and risk levels associated with AI systems.

(5) The Central Government shall empower the IRDC or agencies to establish a knowledge management certification process that verifies the compliance of AI entities with the model standards outlined in this section.

(6) AI entities, upon fulfilling the compliance requirements, may be awarded a knowledge management certification, signifying their adherence to industry best practices in data handling, model governance, and ethical decision-making in AI technology.

(7) AI entities shall be required to submit regular reports to the designated authorities, outlining their adherence to the model standards for knowledge management and decision-making.

(8) The Ministry of Electronics and Information Technology shall establish a regulatory oversight framework to ensure the consistent application and enforcement of these model standards. This framework may involve audits, assessments, and inspections, as deemed necessary.

(9) Failure to adhere to the prescribed model standards for knowledge management and decision-making shall result in penalties and regulatory sanctions, which may include monetary fines, suspension of AI operations, or other regulatory actions as determined by the IRDC.

(10) Repeated or severe violations of these standards may lead to escalated enforcement actions, including the revocation of AI deployment licenses or registrations.

Section 9 - IndiaAI Development & Regulation Council (IDRC)

(1) With effect from such date as the Central Government may, by notification, appoint, there shall be established, for the purposes of this Act, a Council to be called the IndiaAI Development & Regulation Council (IDRC).

(a) The Council shall be constituted as a statutory and regulatory body with a whole-of-government approach to coordinate across government bodies, ministries, and departments;

(b) The Council shall be a body corporate by the name aforesaid, having perpetual succession and a common seal, with power, subject to the provisions of this Bill, to acquire,

hold and dispose of property, both movable and immovable, and to contract and shall, by the said name, sue or be sued;

(c) The headquarters of the Council shall be at such place as the Central Government may notify;

(d) The Council shall consist of a Chairperson and such number of other Members as the Central Government may notify;

(e) The Chairperson and other Members shall be appointed by the Central Government in such manner as may be prescribed;

(f) The Chairperson and other Members shall be a person of ability, integrity and standing who possesses special knowledge or practical experience in the fields of data & artificial intelligence governance, administration or implementation of laws related to social or consumer protection, dispute resolution, information and communication technology, digital economy, law, regulation or techno-regulation, or in any other field which in the opinion of the Central Government may be useful to the Council, and at least one among them shall be an expert in the field of law;

We have not designated the functions of the IDRC, considering this draft bill to be a proposal.

CHAPTER VI: AGREEMENTS AND MONITORING

Section 10 - Guidance Principles for Agreements

(1) The guidance principles are applicable to the following class of agreements related to the use, development and commercialisation of artificial intelligence systems -

(a) AI Software License Agreement (ASLA) –

(i) An AI Software License Agreement shall grant the licensee the right to use AI software in accordance with the terms and conditions of the agreement;

(ii) The agreement should clearly outline the rights and responsibilities of both parties involved in the software licensing process. In principle, the following essentialities may be included in the agreement –

Grant of Rights: The ASLA should clearly define the scope of rights granted to the licensee, including the right to use, modify, and distribute the AI software.

License Restrictions: The ASLA should specify any limitations on the licensee's use of the AI software, such as restrictions on commercial use, modification, or distribution.

Intellectual Property Rights: The ASLA should address ownership of intellectual property rights, including copyright, patents, and trademarks, related to the AI software.

Term and Termination: The ASLA should specify the duration of the license agreement and the conditions under which it can be terminated.

Disclaimer of Warranties: The ASLA should include a disclaimer of warranties, limiting the liability of the software vendor for any defects or errors in the AI software.

Indemnification: The ASLA should specify the extent to which an aggrieved party will be

subject to indemnification, based on the terms and conditions of the agreement.

(b) AI Service Level Agreement (SLA) –

(i) An AI service level agreement (SLA) between a service provider and a customer shall define the level of service provided, including performance metrics, service availability, and service support. In principle, the following essentialities may be included in the agreement –

Service Definition: The SLA should clearly define the scope of services to be provided, including the specific AI functionalities and performance metrics.

Service Availability: The SLA should specify the level of service availability, including uptime guarantees and response times.

Service Support: The SLA should outline the level of technical support to be provided, including response times and escalation procedures.

Performance Monitoring: The SLA should establish mechanisms for monitoring and measuring service performance against agreed-upon metrics.

Change Management: The SLA should address the process for implementing changes to the AI services, including notification requirements and impact assessments.

Problem Resolution: The SLA should define the process for identifying, investigating, and resolving service issues

(c) AI End-User License Agreement (EULA) or AI End-Client License Agreement (ECLA) –

(i) An AI end-user license agreement (EULA) or AI end-client license agreement (ECLA) between a software vendor and an end-user or a client shall respectively legitimise and mutually agree on the control and use of AI software. In principle, the following essentialities may be included in the agreement –

Scope of Use: The EULA or ECLA should clearly define the permitted uses of the AI system, including restrictions on commercial use, modification, or distribution.

User Obligations: The EULA or ECLA should outline the responsibilities of the end-user or client, such as complying with licensing terms and protecting data privacy.

Data Privacy: The EULA or ECLA should address the collection, use, and disclosure of personal data by the AI software, in line with the provisions of the Digital Personal Data Protection Act, 2023.

Intellectual Property Rights: The EULA or ECLA should acknowledge the ownership of intellectual property rights related to the AI software and restrict unauthorized use or infringement at a mutual level.

Disclaimer of Warranties: The EULA or ECLA should include a disclaimer of warranties, limiting the liability of the software vendor for any defects or errors in the AI software.

Limitation of Liability: The EULA or ECLA should limit the liability of the software vendor for damages arising from the use of the AI software.

(d) AI Explainability Agreement –

(i) An AI explainability agreement between software vendors and clients or customers shall require the company (vendor) to provide and submit explanations for the outputs of AI systems. In principles, the following essentialities may be included in the agreement –

Transparency and Explainability: The AI explainability agreement should require the software vendor to provide clear and understandable explanations for the outputs of any class of AI system as listed in Schedule I.

Documentation and Reporting: The agreement should specify the format and frequency of documentation and reporting on the AI system's decision-making processes.

Human Review and Intervention: The agreement should address the role of human review and intervention in the AI system's decision-making processes to examine the reasonably foreseeable misuse of an AI system based on their inherent purpose, means of

classification as per subsection (a)(i) of Section 2 and the risk-based designation as per Section 3.

Continuous Improvement: The agreement should establish and state measures to encourage continuous improvement of the AI system's explainability and transparency.

(2) The guidance principles are consultative and indicative in nature, as may be prescribed.

Section 11 - Post-Deployment Monitoring of High-Risk AI Systems

(1) High-risk AI systems shall be subject to ongoing monitoring and evaluation to ensure their safety, security, and compliance with applicable laws and regulations.

(2) The monitoring and evaluation shall be conducted by the developers, operators, or users of the AI systems, as appropriate.

(3) The IDRC shall develop and establish guidelines for the post-deployment monitoring of high-risk AI systems.

CHAPTER VII: REPORTING AND SHARING

Section 12 - Third-Party Vulnerability Reporting

(1) The IDRC shall establish a secure and accessible platform for third-party vulnerability reporting of risks associated with AI systems. This platform shall allow individuals and organizations to anonymously report vulnerabilities without fear of retaliation.

(2) The IDRC shall establish a vulnerability response team to promptly review and assess reported vulnerabilities. This team shall have the expertise and resources to investigate vulnerabilities, determine their severity, and develop mitigation strategies.

(3) The IDRC shall establish a communication protocol for informing affected parties of identified vulnerabilities and coordinating mitigation efforts. This protocol shall ensure that vulnerabilities are addressed in a timely and effective manner.

Section 13 - Incident Reporting and Mitigation

(1) Developers, operators, and users of AI systems shall have mechanisms in place to report incidents related to AI systems. These mechanisms shall be easily accessible and user-friendly to encourage reporting.

(2) The priority of access will have to be given to incidents related to high-risk AI systems.

(3) The IDRC shall establish a central repository for incident reports.

(4) This repository shall allow for the collection, analysis, and sharing of incident data to identify trends and potential risks.

(5) The IDRC shall develop and publish guidelines for incident reporting and mitigation.

(6) These guidelines shall provide clear and actionable steps for organizations to follow in the event of an AI-related incident.

Guidance Principles for Incident Reporting and Incident Mitigation

We have recommended some guidance principles for incident reporting and incident mitigation independent of the provisions of the draft Bill.

Incident Reporting

- Establish clear reporting mechanisms through measures including having a dedicated incident reporting hotline or a

secure online portal or a designated email address if possible or feasible or necessary
- Encourage timely reporting for timely mitigation
- Provide clear reporting guidelines for AI-related incidents, and mention them in any AI-related agreements and bye-laws
- Protect confidentiality of incident reports

Principles for Incident Mitigation

- Assess the incident and its severity
- Contain the incident by measures involving the isolation of AI systems, disabling specific functionalities and other measures
- Investigate the incident
- Remediate the incident by involving patching software, updating security protocols or retaining employees
- Communicate the incident
- Review and improve incident response procedures

Section 14 - Responsible Information Sharing

(1) Developers, operators, and users of AI systems shall share information in a responsible and ethical manner. This includes ensuring that information is accurate, complete, and relevant to the purpose of sharing.

(2) Information sharing shall be transparent, verifiable, and subject to appropriate safeguards to protect privacy and data security, which includes obtaining informed consent from data principals whose data is being shared.

(3) Data fiduciaries and third-party companies must describe a set of general practices applicable to the developers, operators and users of AI system attributed to information sharing in any

agreement involving the use, development and commercialisation of artificial intelligence technologies.

(4) The IDRC shall develop guidelines for responsible information sharing in the context of AI.

CHAPTER VIII: INTELLECTUAL PROPERTY AND STANDARDS

Section 15 - Intellectual Property Protections

(1) In recognition of the unique challenges and opportunities presented by the development and use of artificial intelligence systems, AI systems must be protected through a combination of existing intellectual property (IP) rights, such as copyright, patents, and design rights, as well as new and evolving IP concepts specifically tailored to address the spatial aspects of AI systems.

(2) The objectives of providing a combination of existing intellectual property rights are –

(a) Encourage innovation in the development of AI systems by providing developers with secure and enforceable rights over their creations and innovations;

(b) Enhance the interoperability of AI systems by ensuring that relevant contractual arrangements are not unduly hindered by IP restrictions;

(c) Promote fair competition in the AI market by preventing the unauthorized appropriation and exploitation of IP assets generated in India;

(d) Protect the privacy and security of individuals by ensuring that the combinations of intellectual property

protections do not compromise the confidentiality and integrity of personal data as per the provisions of the Digital Personal Data Protection Act, 2023;

(3) The IDRC shall establish consultative mechanisms in cooperation with the National Data Management Office and the relevant Centres of Excellence for AI for the identification, protection, and enforcement of intellectual rights. These mechanisms shall address issues such as:

(a) The definition and scope of combinations of intellectual property protections including their limitations as per the legitimate uses designated in the provisions of the Section 7 of the Digital Personal Data Protection Act, 2023 and otherwise as may be prescribed;

(b) The compatibility of such protections with existing IP laws;

(c) The interoperability considerations for the combinations of intellectual property protections;

CHAPTER IX: SECTOR-NEUTRAL & SECTOR-SPECIFIC STANDARDS

Section 16 - Shared Sector-Neutral Standards

The IDRC shall establish a process for developing shared sector-neutral standards for the responsible development, deployment, and use of AI systems.

We have recommended some sector-neutral standards for AI systems independent of the provisions of the draft Bill.

Transparency and Explainability

- AI systems should be designed and developed in a transparent manner, allowing users to understand how they work and how decisions are made.
- AI systems should be able to explain their decisions in a clear and concise manner, allowing users to understand the reasoning behind their outputs.

Fairness and Bias

- AI systems should be regularly monitored for bias and discrimination, and appropriate mitigation measures should be implemented to address any identified issues.

Safety and Security

- AI systems should be designed and developed with safety and security by design & default.
- AI systems should be protected from unauthorized access, modification, or destruction.

Human Control and Oversight

- AI systems should be subject to human control and oversight to ensure that they are used responsibly.
- There should be mechanisms in place for data principals to intervene in the operation of AI systems if necessary.

CHAPTER X: ANTI-COMPETITIVE PRACTICES AND CONTENT

Section 17 - Assessment of Anti-Competitive Practices

(1) In recognition of the potential for artificial intelligence (AI) systems to be used for anti-competitive purposes, the framework

proposed in this Section shall complement and supplement the provisions of the Competition Act, 2002.

(2) The Competition Commission of India (CCI) shall have the primary responsibility for assessing and investigating anti-competitive practices involving AI systems.

Guidance Principles for on AI-related Anti-Competitive Practices

We propose a set of guidance principles for the Competition Commission of India, to examine anti-competitive practices involving AI systems, independent of the contents of this draft Bill.

In assessing and investigating anti-competitive practices involving AI systems, the CCI may consider the following factors:

(a) The nature and extent of market power possessed by AI systems or their developers.

(b) The potential for AI systems to be used to collude, price fix, or engage in other anti-competitive conduct.

(c) The ability of AI systems to collect, analyze, and use data in a manner that may harm competition.

(d) The potential for AI systems to create or reinforce barriers to entry or expansion in markets.

(e) The impact of AI systems on consumer choice, innovation, and economic efficiency.

The CCI shall develop and publish guidelines for assessing and investigating anti-competitive practices involving AI systems. These guidelines shall provide guidance on the factors to consider when assessing anti-competitive conduct, the types of

evidence that may be relevant, and the appropriate remedies for anti-competitive behavior.

The CCI shall monitor and review the impact of AI systems on competition and update its guidelines and enforcement practices as needed to address emerging challenges.

The CCI shall promote public awareness of the potential for anti-competitive practices involving AI systems and encourage individuals and organizations to report suspected anti-competitive conduct.

Section 18 - Content Provenance and Identification

(1) Every AI system, AI that produces an AI-generated content or manipulates content shall have mechanisms in place to identify the source of the content and to maintain a record of the provenance of the content.

(2) This record shall include information such as the date and time the content was generated or manipulated, the identity of the AI system that generated or manipulated the content, and any other relevant information as may be prescribed.

(3) AI systems shall use watermarking to embed identifying information into generated or manipulated content in a manner that is robust to manipulation and that can be used to verify the authenticity of the content and differentiate between AI-generated content and content, which is not produced or manipulated by an AI system.

(4) The watermarking or other identifying information shall be accessible to the public in a transparent manner, which may involve publishing the watermarking or identifying information in a public repository or making it available through an open API.

(5) The IDRC shall develop and publish guidelines for the implementation and use of watermarking and other identifying techniques in AI systems.

(6) These guidelines shall address issues such as –

(i) the type of information to be embedded in watermarks;

(ii) the robustness of watermarking techniques; and

(iii) the accessibility of watermarking information.

(7) The IDRC shall certify the use of watermarking techniques in AI systems and assess the effectiveness of these techniques in preventing the misuse of AI-generated content.

(8) The provisions of this Section shall apply to all AI systems that generate or manipulate content, regardless of the purpose or intended use of the content, including those AI systems that generate text, images, audio, or video.

CHAPTER XI: EMPLOYMENT AND INSURANCE

Section 19 - Employment and Skill Security Standards

(1) Employment Security

(i) Companies or entities employing high-risk AI systems shall not reduce human employment opportunities without implementing safeguards to protect the rights and livelihood of affected employees.

(ii) Employers deploying high-risk AI systems shall engage in consultation with their employees and relevant employee representatives to establish fair transition plans that may include retraining, redeployment, or alternative employment opportunities.

(iii) The Ministry of Labour and Employment, in collaboration with the Ministry of Electronics and Information Technology, shall prescribe detailed guidelines for employment security in the context of AI technology deployment, emphasizing fair labour practices.

(2) Skill Security

(i) Companies or institutions actively involved in the development, application, or research of AI technologies shall facilitate skill development initiatives for their workforce and, where appropriate, offer training programs for acquiring new skills.

(ii) Sector-specific skill development programs and vocational training centres shall be promoted to address the evolving skill requirements arising from AI technology advancements.

(iii) The National Skill Development Corporation (NSDC) and sector-specific Skill Councils shall collaborate with the Ministry of Skill Development and Entrepreneurship to define skill development standards and certifications tailored to the AI sector's demands subject to the National Occupational Standards and Qualification Packs, and even otherwise as may be prescribed.

Section 20 - Insurance Policy for AI Technologies

(1) Any organization or entity that develops, deploys, or utilizes high-risk AI systems shall be mandated to obtain comprehensive insurance coverage to manage and mitigate potential risks associated with AI operations.

(2) The Insurance Regulatory and Development Authority of India (IRDAI) shall, in conjunction with relevant ministries,

specify the minimum insurance coverage standards for AI technologies. The insurance coverage requirements shall encompass –

(i) technical failures;

(ii) data breaches; and

(iii) accidents,

(3) Entities deploying AI systems must maintain records of their insurance policies, ensuring that these policies cover a comprehensive spectrum of AI-related risks and liabilities.

(4) Insurance companies offering AI technology coverage shall operate within the guidelines and directives laid out by the IRDAI.

(5) The IRDAI shall establish rigorous underwriting criteria and risk assessment procedures specific to AI-related insurance policies, which shall encompass –

(i) assessment methods;

(ii) premium calculation models; and

(iii) claims processing standards.

(6) Insurance providers shall be responsible for presenting transparent and detailed insurance policies tailored to the unique risks of AI technologies, and they must promptly address claims and compensate policyholders as per the policy terms.

(7) Entities deploying AI systems shall be obligated to furnish evidence of their insurance coverage when procuring or deploying high-risk AI systems.

(8) The Central Government, through the Ministry of Electronics and Information Technology, may necessitate AI entities to furnish periodic reports on their insurance policies, including claims made and settled.

(9) Failure to comply with the insurance requirements outlined in this section shall subject the AI entity to monetary fines and potential regulatory sanctions as per the discretion of the Central Government.

CHAPTER XII: APPEAL AND ALTERNATIVE DISPUTE RESOLUTION

Section 21 – Appeal to Appellate Tribunal

(1) Any person aggrieved by an order or direction made by the IRDC under this Bill may prefer an appeal before the Appellate Tribunal.

(2) Every appeal under sub-section (1) shall be filed within a period of ninety days from the date of receipt of the order or direction appealed against and it shall be in such form and manner and shall be accompanied by such fee as may be prescribed.

(3) The Appellate Tribunal may entertain an appeal after the expiry of the period specified in sub-section (2), if it is satisfied that there was sufficient cause for not preferring the appeal within that period.

(4) On receipt of an appeal under sub-section (1), the Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

(5) The Appellate Tribunal shall send a copy of every order made by it to the Board and to the parties to the appeal.

(6) The appeal filed before the Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within nine months from the date on which the appeal is presented to it.

(7) Where any appeal under sub-section (6) could not be disposed of within the period of nine months, the Appellate Tribunal shall record its reasons in writing for not disposing of the appeal within that period.

(8) Without prejudice to the provisions of section 14A and section 16 of the Telecom Regulatory Authority of India Act, 1997, the Appellate Tribunal shall deal with an appeal under this section in accordance with such procedure as may be prescribed.

(9) Where an appeal is filed against the orders of the Appellate Tribunal under this Bill, the provisions of section 18 of the Telecom Regulatory Authority of India Act, 1997 shall apply.

(10) In respect of appeals filed under the provisions of this Bill, the Appellate Tribunal shall, as far as practicable, function as a digital office, with the receipt of appeal, hearing and pronouncement of decisions in respect of the same being digital by design.

Section 22 – Orders passed by Appellate Tribunal to ne executable as decree

(1) An order passed by the Appellate Tribunal under this Bill shall be executable by it as a decree of civil court, and for this purpose, the Appellate Tribunal shall have all the powers of a civil court.

(2) Notwithstanding anything contained in sub-section (1), the Appellate Tribunal may transmit any order made by it to a civil court having local jurisdiction and such civil court shall execute the order as if it were a decree made by that court.

Section 23 – Alternate Dispute Resolution

If the IRDC is of the opinion that any complaint may be resolved by mediation, it may direct the parties concerned to attempt resolution of the dispute through such mediation by such mediator as the parties may mutually agree upon, or as provided for under any law for the time being in force in India.

We have provided a list of suggested provisions, which may be expected in the draft Bill, but do not have any substantive necessity to be drafted.

CHAPTER XIII: MISCELLANEOUS

Section 21 - Power to Make Rules

Section 22 - Power to Make Regulations

Section 23 - Protection of Action Taken in Good Faith

Section 24 - Offenses and Penalties

CHAPTER XIII: REPEAL AND SAVINGS

Section 25 - Savings Clause

CHAPTER XV: FINAL PROVISIONS

Section 26 - Power to Remove Difficulties

Section 27 - Amendment of [Other Legislation]

SCHEDULES

We propose that the schedules as described in the draft Bill must cover the following contents as proposed:

Schedule I: Applicable Laws which are sector-specific, sector-neutral and related to the substantive aspects of the draft Bill.

Schedule II: List of Strategic Industry Sectors

Schedule III: List of Classes of Artificial Intelligence Technologies in a Table

Annex: Additional Recommendations on Strategizing AI from our Technical Reports

We have presented some of the recommendations as quoted and proposed in the technical reports and publications developed by **Indic Pacific Legal Research** & its member organizations, including the **Indian Society of Artificial Intelligence and Law**. These recommendations and policy suggestions are produced in the context of the publications developed in the years **2020-2023** and have academic and industry-oriented perspectives. *We express our gratitude to the young and talented law and policy professionals across the country, for their invaluable insights.*

2020 Handbook on AI and International Law [RHB 2020 ISAIL] (2020)

Chapter 1

- AI Ethics is highly dependent on the kind of industry it is involved with & the cultural and anthropological aspects of the society and individual spaces which encourage the industries to sustain.
- Some aspect of AI Ethics is also based on information warfare, because of the fact that much hype [...] which is created on the use and impact of AI as a product/service decently affects the market conditions. Even due to a great lack of research on the effectiveness of AI, despite the fact that the quantity of AI papers published has increased much since 2017, narratives are made which may affect justice administration and rule of law in ascertaining the role of AI Ethics as a soft law.
- It is therefore reasonable to ascertain that AI Ethics as a soft law would be helpful enough to render approaches towards ideation in matters related to policymaking.

- Generally, surveillance activities, private censorship on social media platforms, health-related surveillance, recognition software-based verification and other related activities come in the scope of algorithmic policing. It is therefore important to understand that algorithms-based policing of activities must be based on transparent enquiry, and the use of such technology must be reasonably scrutinized in order to avoid any mishandling, considering the delicate nature of the practice.
- Algorithms generally can be used to ensure means of warfare in cyberspace (disinformation warfare, cybercrimes, etc.) or in physical space again through algorithmic activities. Currently there is no regulation of algorithms-based warfare in international law. Using data of users, whether any, to feed algorithms in order to cause private censorship is also algorithmic warfare. Algorithmic diplomacy therefore diplomatic negotiations on the basis of policy, legal, strategic and political intervention of algorithms. Bargaining and conciliation, often in the matters of fintech-based trade, or IP rights or digital rights can be done using this generation of diplomacy considering the integral role of AI/ML systems in the foreign relations between countries and non-state actors.
- The intersectional role of management sciences, social sciences and special sciences enables thought leadership and education activities in the field of AI Ethics principally. Now, a basic model of learning and education in AI Ethics and Policy to include other important fields, which we add up or mix with, can be in the form of AI+X, where X means any field possible, which can be put into parallel use with AI Ethics.

- In generic conjunction, it is important to understand that Artificial Intelligence can be understood as (a) a concept; (b) an entity; or even an (c) industry. As a concept, AI contributes in developing the field of international technology law prominently, considering the integral nature of the concept with the field of technology sciences. We also know that scholarly research is in course with regards to acknowledging and ascertaining how AI is relatable and connected to fields like international intellectual property law, international privacy law, international human rights law & international cyber law. Thus, as a concept, it is clear to infer that AI has to be accepted in the best possible ways, which serves better checks and balances, and concept of jurisdiction, whether international or transnational, is suitably established and encouraged.
- As an entity, questions have been largely on the entitative status of AI. Since, AI is an abstract concept, as an entity, autonomous vehicles, robots, facial recognition systems, etc., are within the practical and tangible categories of what constitutes an AI. Some laws and regulations mention the term not as AI but as algorithmic systems, autonomous systems, automated systems and so on. We would be using the term 'AI' in a loose fashion throughout this book, but with a purpose that the chapters serve a reasonable cause in teaching and explaining how AI is recognized legally. On the question of the entitative status of AI, under jurisprudence, there can be 2 distinctions on a prima facie basis: (1) the legal status; and (2) the juristic status. The former relates to the idea that a competent authority, i.e., either a state (through its legislative wing or the executive wing) or a treaty body/intergovernmental organization can effectively draft a law (regulation, treaty, declaration, covenant, constitutional amendment, rule etc.,). Obviously, in the case

of an international organization, the process differs as accession to ratify/signature to ratify is something that countries have to decide. At national jurisdictions, governments can enact laws on recognizing the status of AI as well, which effectively forms an important trend or part of the state practice recognized under international law. The latter status is quite different. It is not that governments or international organizations cannot have a say here, but the recognition here would-be fluid and interpretive. Most of the time, it is the quasi-judicial bodies, expert groups, standing committees and even the courts, which decide the juristic status of something. Traditionally, here in the case of AI, this would be an appropriate method, but reckoning it is not exactly as legalistic as in the former case it would be.

- AI as an Industry is a tricky territory, which has to nurture and evolve with the changing times. Now, it is the state primarily, which decides how it develops and maintains its economic and social interests. AI's usage at an industrial level is imminent, considering the fact that it has its own importance in both the hard power and soft power aspects of the state. In the domain of hard power, AI can be used for cutting-edge defence tech, surveillance etc., while in the domain of soft power, AI can be used for public censorship, biometric and facial recognition, etc.
- We need to treat AI's omnipotence and omnipresence whether as a legal entity or as a juristic entity. Omnipotence generally refers to the all-comprehensive and expansive abilities of an entity. Omnipresence, on the other hand refers to the all-comprehensive and expansive presence of an entity. So, when we discuss AI's omnipotence – it has to do with the fact that business leaders and tech giants generally support the notion that AI should be all-invincible to avoid any risks in its activities and operations (Arbitral.com; Stewart, 1993). AI's omnipresence therefore is about the test of outreach, influence & the constructive

precautions behind the wide reach and utility of the AI-based product or service, which includes its ramifications.

- As a concept, countries might have different scholarly views on AI's omnipresence and omnipotence. However, based on juristic interpretation, it has to be seen effectively how such practices are recognized as state practice, which might ought to be reckoned as a constituent element of international legal custom;
- As an entity, a focus would be more on the legal status of AI, but the vicarious effect of actions and operations led by or through AI-based products and services would define the cardinal aspect of corporate liability, since on a dominant basis, the principle of agency will be of utmost focus here;
- As an industry, there can be some principled agreements among countries on the principles regarding human rights and liberties & how AI's omnipresence and omnipotence can influence it, but even if that is possible, there should be more anthropological focus on how industries drive narratives and research on this aspect of AI Ethics, because here, the role and accountability of private actors, startups etc., would be of utmost importance. Sovereignty also would be importantly defined;

- The economic and social utility of AI will always be put under question, because more or less, it would be a policy question, therefore reserving the matter to the executive and parliamentary branch of the governments. Additionally, intergovernmental organizations and expert groups should have a say, but only for suggestive reasons. Consultative recognition of the economic and developmental angle of AI's recognition and agency would differ in the three categories as follows:

- As a concept, focus should be more on the development and practice of the field, which is academically factual and non-partisan & constructive. Intellectual harmony in the schools of thought always invites better contribution in the literature of international law and artificial intelligence. The factor that AI has different utilities and presence depending on the kind of product/services involved also affects the scholarly position;
- As an entity, the direct and indirect effects of actions and operations of AI would be put into question, and the principle of agency will be an important focal point for the purpose of adjudication and risk assessment;
- As an industry, the economic and social utility of AI has to be in consensus with the three factors: (1) state consequentialism or state interests; (2) industrial motives and interests; and (3) the explanability and reasonability behind the industrial products and services central or related to AI;

- Auditing of AI as a concept is as cogent and clearly needed among countries, because it enables companies and governments to measure and safeguard recognition of risk assessment and operations led through AI. Having international standards for auditing AI as an entity again would invite a new uncharted territory of question: How can the liabilities and responsibilities of AI as a product or a service or a reckoned entity (system) can be audited at an international level. Industry-wise auditing also is legally reasonable at subsidiary levels, and can be uniform at substantive levels;
- As a legal entity, the genealogy behind the concept of rights, liabilities and duties changes. The concept of agency of AI as a product/service is the current practical means to assure corporate liability, but the anthropological basis of absolving

from agency-based liability would radically differ based on the kind of AI being put into use.

Chapter 4

- Since consequentialism in AI Ethics might have its own fatal setbacks as discussed before, it is suggested that the democratization of AI must be seen in a cyclic manner, with distributive and decentralized goals, which do not emphasize on the tendency to replace a status quo through external or third- party measures. Internal democracy is important among communities, companies and organizations, which emphasize upon short-term and long- term goals, which are not limited to myopic visions and goals like artificial general intelligence (AGI), for example, but are beyond that, based on research, academic creativity and freedom of expression to individual and collective entities. Therefore, democratizing innovation and the course of innovation in AI would also require introspection.

Chapter 7

- First and foremost, it is extremely imperative to understand that AI is something which aids humans and AI has been proven to help and aid individuals in understanding their intellectual property rights. For instance, the use of AI in the administrative levels of Intellectual Property Rights can be made much simpler and easier with the use of machine learning techniques which could be deployed when it comes to the administration of the innumerable applications which fall under the garb of IP protection. One such example is the World Intellectual Property Organisation's Translate and its Brand Image Search software.

- The second aspect which needs to be covered here is with regards to how intellectual property can be deemed to be regarded as a part of the legal system which has the capacity to protect AI. AI tools and various ML techniques are already being deployed in the justice system in a number of jurisdictions, however, the introduction of these autonomous tools in the justice system is ought to create a number or a series of significant impacts upon the creation, production and distribution of cultural goods and services. In fact, it can safely be said that the policies that are envisioned within the scope and the ambit of IP laws are aimed towards fostering innovation and creativity in the economic and technological sphere- this is where AI and IP laws merge and intersect with each other.
- Yet another serious question that arises here is whether the individual who files for a patent application, attempting to patent his AI innovation be deemed to be regarded as an owner of the patent or not, and whether there are enough provisions within the various international legislatures which have the capacity to grant IP protection to innovation which are autonomous or created by way of an AI application. Furthermore, it can be safely said that when it comes to the interpretation of patents, the aspects with regards to an inventive setup or non-obviousness are ought to arise. Lastly, the various conditions pertaining to the clauses of disclosure can be deemed to be regarded as an extremely strenuous task when dealing with inventions which are a result of an AI application. The primary concerns that arise here are how can disclosures be fulfilled when the algorithms which are powered into the AI devices constantly change over time, in fact, it can be an extremely arduous task when it comes to an AI software that is powered or that runs on "black-box" algorithm, which is something that cannot be identified easily, which leads to the question

as to whether an AI application which runs on black-box algorithm can be granted IP protection or not.

Chapter 8

- A lot of experts are of the opinion that the AI systems are extremely complicated and can never be completely protected. The ultimate risk that arises here is with regards to the fact that risk management does not have the perfect potential to detect whether there exists a "kill-switch" option in a system that is being run and whether such an option can be activated at times of an international armed conflict or an accident or an emergency or during the lockdown of an AI infrastructure which is extremely crucial in nature, for instance, tele-communication. Consequently, there also looms a risk with regards to the disclosure of certain intellectual property which may again render the privacy of a country vulnerable or put the national secrets in jeopardy, or perhaps in the wrong hands. It is extremely imperative to understand that the role which AI plays needs to be framed in such a way that it helps to erase the existence of a kill-switch or protects the intellectual property of a country.
- Furthermore, the legitimacy of a code of control can be challenged inter alia. The algorithms which are programmed in the various software's used by a country, usually have an intellectual property value and they cannot be inspected properly, since usually these algorithms are developed by other private organizations who have their intellectual property rights in place. In fact, an AI, which is based on a neural network does not have the capacity to make a decision and this could possibly render the data vulnerable. Therefore, when it comes to taking a risk-based approach or a risk management approach, it is extremely necessary to understand that such an approach may render the data vulnerable and perhaps may lead to the occurrence of a host

of issues, which may not be in consonance to the ethical or legal principles of a nation, which may not be because of the extensive use of AI, however, the usage of AI will make such a perspective unethical in nature.

Chapter 10

- Albeit the fact that wide and extensive application of [the artificial intelligence] technologies have already been deployed in the global environment, the scheme of international environmental law has failed to support it adequately. Specialised agencies of the United Nations such as the United Nations Environment Programme, International Maritime Organisation, United Nations Framework Convention on Climate Change and World Meteorological Organisation have shown active support through artificial intelligence development projects in recent year. [...] Despite this, multilateral initiatives in respect to artificial intelligence in the global environment are almost non- existent and only few General Assembly Resolutions exist in the sphere (Law Library of Congress, 2019). The Organisation of American States, European Union and the Council of Europe have formed few regional instruments, but they seem to be generic in nature and do not deal with specific artificial intelligence technologies in its application to the global environment.

Chapter 11

- Although origins of convergence in the global energy sector with artificial intelligence can be traced back to the 1980s, regulatory mechanisms in the international sphere have been lackadaisical. This is mainly due to the fact that there are extremely few public international law conventional instruments in the sector and most of the global energy sector is regulated by private international law investment

treaties and agreements. The looming cyberthreats and vulnerabilities of the artificial intelligence technologies that have severely affected the global energy sector over the years have also shown the need for lawmaking. Not only this, but the claim that artificially intelligent enabled tools and technologies are capable of reducing emissions and can enhance clean energy sources are itself challenged since these technologies themselves use humongous levels of energy to operate.

- Moreover, the fact that most developers are either private sector companies or researchers from Universities and that, Government affiliated developers are rare, the need for sufficient multilateral, bilateral and regional legal instruments for capacity building, investment incentivisation, increased and cross- border development done keeping in mind relevant national standards and issues revolving around artificial intelligence technologies is currently the need of these times.

Chapter 12

- It seems to be clear that the involvement of Governments and Government- affiliated organisations have been significant in the expansion and development of the space sector. Despite this fact, all the multilateral legal instruments signed by Governments do not directly pertain to artificial intelligence technologies in any manner and only seem to focus on the general principles and law required for smooth development of the space sector. Looking at the rate of space commercialisation, the non- existence of a robust international framework which deals with all the aspects related to use of artificial intelligence in space may open Pandora's box in the near future.

Chapter 13

- Some artificially intelligent tools, software and platforms have also been combined with non- artificial intelligence fourth industrial revolution technologies such as the internet of things, big data analytics, virtual reality, augmented reality and cloud computing to achieve their objectives. In fact, some technologies have also seen synthesis between artificially intelligent software and hardware, especially in cases of self- check in kiosks, baggage and security scanners, autonomous robots, autonomous vehicles and self- driving wheelchairs. The results above also showcase that artificial intelligence technologies have not been sufficiently developed for some civil aviation related activities such as training of pilots, fleet management and crew management and minimum amount of technology exists in this sphere. Furthermore, artificial intelligence technologies which enhance sustainability in aviation only focus on the fuel efficiency aspect and ignore various other sustainability related aspects.

Chapter 15

- Fissuring is the act of migration of jobs or outsourcing of jobs to contractors who perform those tasks for a cost that is lower than what the business was paying for it when it was integrated within the business. When automation and fissuring are compared it can be inferred that the simple reason for resorting to either of those practices depends whether they reduce the overall cost of operations without sacrificing the efficiency of the organization or not. Fissuring is not just bad for the workers that were employed at the business, it is no bed of roses for the replacement workers who are employed at the outsourcing companies either. Because of the tough competition and non- adherence to labour standards, their companies are compelled to cut

costs in whatever way they can. This results in erosion of labour standards and decline in wages and also allows for companies to save money through illegal means by not complying with regulatory practices.

- There are two kinds of fissuring which policy makers need to be worried about: outsourcing jobs to countries where the manufacturing of the product is more cost effective or the labour for the service rendered is cheap and the conversion of actual jobs into gigs and the hiring of employees on a contractual basis. Outsourcing of work to different countries allows the businesses to benefit from cheaper labour costs benefit from, weaker regulatory mechanisms and depressed union standards.
- The policy and regulatory approach to deal with automation will have to acknowledge the existing legal framework for labour and the disadvantages which burden it in comparison to automation, as discussed earlier one of them is the worker benefits and labour standards which the employers have to adhere to adding to the costs of the business. This legal framework which is there to protect the workers is the cause of businesses resorting to automation and outsourcing.
- Even though a parallel can be drawn between automation and fissuring when it comes the comes to the reasons as to why the business would opt one or the other, instead of employing a human workforce for their business, automation has a big advantage over fissuring when it comes minimizing the cost of the business. Automation results in a complete substitution of the human workforce and provides the employer with a absolute free pass from bearing the costs, risks, and difficulties of employing people, including those that arise from the law of work unlike fissuring which only provides for a partial solution.
- With the development of technology resulting in cheaper costing software's and robots, and ever so increasing cognitive abilities of AI because of continuous cloud-based

machine learning, they will outpace human skill and cost effectiveness in no time. The organizational innovations that come under the rubric of fissuring, though aided by technology, still have to rely on human performance and while also managing the cost of sustaining human beings and reproducing their labour. Automation overcomes both of these requirements. It offers firms the ultimate exit from bearing the cost of human employment and also eliminates all the indirect costs which the employer had to bear in the form of reduction of workers' exposure to occupational illness or injury, discrimination, retaliation, and excessive hours. Because of such obvious advantages of automation and fissuring over conventional employment, there is a major predicament which exists when developing a response to those two issues. Many scholars have argued on prohibitions against fissuring or automation and creation of a legal fortress of employment, expanding the rights and duties which are to be borne by the employer and extend such duties to the labour which the firm is employing via means of fissuring. But such a solution would again increase the cost of employment and lead employers towards automation. Hence it can be concluded that any proposal to expand the responsibility of the employer would drive them away from employing humans.

- Dehumanization occurs when an individual views another person in negative ways, which leads to the belief that the other person is undeserving of the respect and kindness usually afforded to oneself and another person [...]. The use of robotics or other IT tools which work alongside humans runs the risk of dehumanizing their work because it can just be viewed as an extension of the robot or the IT tool itself. This has very bad impact on the perception of labour being performed by humans and the work which they perform is not treated with the same dignity as any other work which humans perform and is also depreciated in valued.

- The advent of AI enabled surveillance devices has made it very easy for companies to amass a huge amount of information on their employees in both professional workspaces and intimate spaces. Such over the top forms of surveillance can also lead to increased worker stress and decreased productivity [...]. Because the working of these systems is unknown to the individual who is being made subject to such technologies, you can never know whether the said system is affected by any explicit or implicit biases or not. For example, the software might be too productivity focused and might exclude people with disabilities from employment. Thus, it can be said that management by algorithm because it lacks sensitivities which are akin to human minds might not lead to desirable outcome in workplaces. Because the machines and algorithms are working with very narrow notions of efficiency and productivity, they fail to take into account into account the numerous hidden costs associated with schedule instability and produce suboptimal results for the business.

Chapter 20

- Reliability and dependability is just one phase of the much bigger horizon while interacting with machines and self learning automated devices. These automated or AI devices could conquer the ability to harness the data, trust and intelligence to achieve its object under any circumstances. If an AI device is made to record surrounding noises, then depending on the algorithmic design, it could configure itself to reduce its hardware functions, save energy and increase the recording capabilities even after switching it off manually. This configuration could also be self-optimized to go against human will and discretion very easily. The bottom line remains, once technology starts playing greater role in lives, we would get more attached to it and lay greater trust

in it. It is not entirely an unacceptable or wrong happening, the concern only remains that laying trust rapidly on algorithmic decision making without a system of checks and balances is a step in the wrong direction. Although with such a system as well, algorithmic decision making and extreme blind trust is something to be wary about.

- AI can resemble itself as a Subject to any activity or operation in an environment. The relationship between AI and human rights law establishes when the effect of AI being a subject is characteristically involved in the emanative cause to enforce, adjudicate, maintain or recognize a human right.
- If there is no emanative cause directed at humans as objects, establishing the relationship would be unreasonable;

    - AI can resemble itself as an Object to any subject, like humans. GDPR recognizes the rights of the data subjects, for example (humans), and so forth there should not be any generic problem in establishing any AI-human rights relationship. There is ongoing research on such a relationship already;

    - AI as a Third Party is an interesting uncharted legal territory. When we recognize AI as a third party, in human rights law enforcement issues, we have to recognize the fact that this correlation is quite inexplicable if the entitative status of AI is not clarified. Although, in the interpretation of AI being an entity, there is no disagreement in accepting that there can be two possible notions: either AI is an electronic legal personality [...], for example or it can be under some form of possible agency, thereby establishing the legal formula of corporal liability where liability stands over the developers, manufacturers, company executives etc., who exist under the clout of principal of the AI agent.

However, while the former case is uncharted, and the latter case may not, let us be clear that as a third party, AI's treatment as a legal/juristic personality has to be personified in some reasonable manner to establish the relationship between AI and human rights law. It can also be argued that the third-party scenario is a middle scenario between AI being a Subject and AI being an object;

- However, in either of the 3 examples, the subject-matter, which is AI, will be essentially important because even if on principle, a technical relationship can be established, in practice cum experience, it would not be possible to do the same unless we are clear with what kind of AI is being utilized. So, AI is again conceptually abstract despite having its different definitions and concepts. Also, there are different kinds of products and services, where AI can be present or manifestly available either as a Subject, an Object or that manifest availability is convincing enough to prove that AI resembles or at least vicariously or principally represents itself as a Third Party. Therefore, you need that SOTP classification initially to test the manifest availability of AI (you can do it through analyzing the systemic features of the product/service simply or the ML project), which is then followed by a generic legal interpretation to decide it would be a Subject/an Object/a Third Party (meaning using the SOTP classification again to decide the legal recourse of the AI as a legal/juristic entity). Let us understand why the idea of 'manifest availability' is important.
- Since AI is conceptually abstract, it is important to understand that in practice, algorithmic activities render different tools which can be considered as AI.
- Data quality as a concept is also involved in the foot-printing of human identity (or digital foot-printing so we say). Digital foot-printing, its history, maintenance and its trends are

essential for any forensic / intelligence / risk assessment to estimate the congenial and foreseeable impact AI can probably have upon the mandate and principled responsibility of the state to ensure that human rights are safeguarded at the first place.

- Generally, the role of the conception could be limited to normal data collection and storage activities, but here, while human rights jurisprudence does not have much clear role, because the concept focuses on a clear and tangible enforcement of legal rights, the principle of Privacy by Design (& Default) would surely enable a clear cause for human rights law interpretation because:

    - In the case of artificial intelligence-based products and services, the dynamic and obscure characteristics of AI, which are manifestly available would surely be reflective when it would be required for the principal/company to prove that effective measures under the same principle were taken to ensure that privacy by default and design is systemically safer;
    - Data storage would never be a human rights issue; it is purely a legal concern. However, the systemic congeniality of the pseudonymization infrastructure is very important here, and it cannot be ignored. Other than the fact that AI is dynamic and is manifestly available, the technological semblance between the algorithms (and their operations/activities) & the pseudonymized infrastructure would be tested;

- Algorithms must be assessed on the basis of the life-cycle of the AI product/service and the activities/operations they undergo. A robust legal framework of algorithmic accountability is therefore important. The concept of Responsible AI on the other hand is helpful because it defines how companies/private

entities/trusts/NGOs/other entities and governments would shape the notion of responsibility, accountability and liability, thereby very importantly contributing in the notions of customary international human rights law on the effects of algorithmic activities and operations on the human rights of data subjects;

- The idea of Explainable AI or XAI is essential because explicability of disruptive technology in the field of human rights does not limit itself with the legal obligation to be transparent, but also extends to reflect how algorithmic operations/activities attribute their effects on the human data subject. A take could be that the fault lines of an AI proved by its explicability could show the systemic biases within the system. However, the take is of no use in consideration because biases, human and algorithmic, are natural and strategic. It is therefore more of a policy and enforcement issue, and not a legalistic issue, where subjective or abstract interpretations on the relationship between AI and human rights can be easily established. XAI – if leads to algorithmic transparency would then invite more anthropological study on the way any manifestly available AI talks to human data subject through the genealogy and quality of data & the privacy of design (and default) that it possesses;
- Liberty is at the heart of human rights, which itself has to be understood through some anthropomorphic context, because the cluster of rights, when is recognized and revered, is always accepted within a human undertaking or understanding of things and subject-matters. Therefore, a concept of machinic empathy [...] also comes into play, which is important for anyone to understand how the ontological words of human and AI environments talk to each other and converse;
- We can also interpret this in the following way: imparting a limited form of intelligence (since for example the term robot

has its origins to the world slav, meaning slaves, hence limiting the aesthetic scope of robots for industrial work or work 'equivalent to that of workers') has a cultural and knowledge sharing aspect too, which in turn affects the way we understand right to life. Therefore, adding to the point of machinic empathy, it is clear that this form of cultural congeniality might be tested as well;

- Expression enables creativity, feedback and conversational-collaborative governance. Considering the lack of machinic empathy, which can exist in AI products and services, and the chances of algorithmic discrimination that can happen [...], it has to be established clearly that the regulation of hate speech, and even its classification, should be limited within the scope of the state [...] . For example, social media platforms are becoming public utility platforms (if not all, then at least platforms led by big tech companies, for example, Google, Facebook, Twitter, etc.,), which owes to the coherent need of cyberspace for the basic necessities of people. It therefore is important that the freedom of expression under international human rights law is protected and respected. At the same time, it is essential that the regulation of free speech is vested with the states and not companies.
- The factor of machinic empathy, adding the aspect of SOTP classification of AI products and services, would affect choice rights in international law. Since establishing liability on algorithmic operations/activities requires reasonable state intervention, it is important to establish that the different intersectional and transpiring activities emerge due to the human rights which are exercised by human data subjects, taking into consideration the omnipresent and all-cohesive behaviour of disruptive technologies , there is no doubt that the finite and basic aspects behind the exercised and recognized human rights (or constitutional rights in a national context) must be protected. Additionally, the

intersectional and transpiring activities generally enable people to exercise to have a right to choose;

- Now, choice rights, can be identitarian, or proceduralist, or substantive, based on the kind of preferences (legal), which are available. Choice rights can be available in any possible scenario: (1) economics when it comes to buying products and taking services (reference to anti-trust law issues); (2) political freedoms with privity and privacy against surveillance and political correctness assumed by third parties; (3) creative freedoms against cyber contamination and shadow bans; and many more;

Chapter 21

- AI Ethics is an important and strategic part of technology policies, which reflects the national, foreign and internal priorities of the government's interests to democratize and utilize the technology for economic, diplomatic and other legitimate causes;
- AI Ethics is self-reflective to the cultural nature of societies and civilizations, because they just not only represent the needs and trends of a country and its people, but also reflect how such measures are proportionately applied and put into the best use possible;
- AI Ethics resembles the constitutional, civilizational and public value systems as well (both moral and ethical). It is by the virtue of technology ethics that we can estimate how cultural relations and culture-inspired strategic intrusions can be made, because AI bridges the connectivity between physical spaces, cyber/digital spaces & the space of information & perception warfare;
- In terms of implementing, respecting and expanding the juridical scope and relevance of international technology law, AI Ethics indeed has an important role, as it defines the emerging trajectories in technology ethics and

jurisprudence. States can opt for monistic or dualistic approaches in wherever possible steps they undertake, which also is contributory to the development of multilateralism;

- Identity is an important aspect of the political relevance of technology in the realpolitik. Identities can be of many kinds, and their structural formations also do differ, but AI explanability would be essentially important in the context of international cultural law.
- Explanability offers a serious opportunity to understand how indifferently/differently human actors and the manifestly available AI understand and process points of identity. This stems beyond the question of privacy of design & default, because here, a real estimate of AI's explanability can probably explain how the manifest availability and utilization of AI offers possible considerations over ensuring that cultural and individual liberties are protected;
- Towards the angle of policy, identities can be used dynamically. Like TikTok, applications, for example can be used to target practices or activities, which may amount to ethnocentrism or cultural appropriation. If effective policies are developed on the relevance and transformation of XAI policies in the perspective of identity-based or identity-centric algorithmic activities and operations, then the technocratic democratization of cyberspace can be tackled in a reasonable manner;

Regulatory Sovereignty in India: Indigenizing Competition-Technology Approaches, ISAIL-TR-001 (2021)

- Deriving from not only academic resources, but also through boots-on-the-ground work & surveys – is the approach that needs to be taken with regards to governance in technology law. If Coherentist approaches are needed - it is important

for the legislators to understand at the grassroot level - the implications of the same. If a technocratic approach is preferred, the domestic policy coordinates must be calibrated with some precision to gain leverage in the international community, which needs to be taken into consideration.

- In case of *Regulatory-Instrumentalist approaches*, regulations need to be kept in check by bodies to ensure practical if not idealistic working of the machinery.
- Mechanisms for addressing & evaluating how technological platforms are able to take advantage of consumer biases & allocate consumers to their platform by creating difficulties for them to switch to alternatives.
- There should be a test of assessing Permeable Indigeneity in Policy (PIP). This concept, simply means, in proposition through this report that whatsoever legal and policy changes happen, they must be reflective, and largely circumscribing of the policy realities of the country. PIP cannot be a set of predetermined cases of indigeneity in a puritan or reductionist fashion, because in both of such cases, the nuance of being manifestly unique from the very churning of policy analysis, deconstruction & understanding, is irrevocably (and maybe in some cases, not irrevocably) lost. Thus, we strongly recommend that PIP must be determined by determining that manifest reality in the following phases:

  a. Decide a specific subject-matter
  b. Check how much and what policy-matter is derivable or discoverable from the subject-matter decided. Once that is done, PIP cannot be extra-terrestrial or extravagant. It must be specific, even if largely related while a fashion of policy determination is accepted while some critical output is discovered/derived.
  c. Apply your thought processes/design thinking approaches and see how much amorphous and not reduced/deciphered form of indigeneity as a policy

phenomenon in the environment is derived/discovered. In simple terms, how much complex adaptivity is discovered, which led you to conclude that manifest derivation/discovery.

d. Now the derivation should not be considered indigenous, from a point of view whether it has pure cultural origins, but from whether the environment from where such derivation/discovery has happened relates to that kind of indigeneity to the policy itself. It means that something indigenous here is not being used in the context of cultural heritage in general, but in the case of policy realism, whether that derivation/discovery reflects and even in a real-time scenario, emulates the policy phenomenon. It is a different case that the phenomenon and the derivation/discovery, might be related with distinctive aspects of cultural conundrums, or historical assets per se. Since, we are dealing with how to become creative in making policies or seeking better policy ideas, the motive is not to focus on issues of research in anthropology, history, archaeology, sociology, and other fields related to, simply because we cannot opt a reductionist/puritan approach in policy determinism ab initio and ad infinitum.

e. This also does not mean that design models based on Indic Knowledge Systems cannot be created ever. IKS can always be a complementary and suggestive field, which as relates or contributes largely to the design thinking approaches to derive/discover outputs, could render its own amorphous salience, and pragmatic value. This could be a much practical way to incorporate IKS in the field of technology law and policy, in general.

- Policy maturity comes by realising that derivation/discovery is at least done. When AI Ethics, is understood, and the

intersectionality is developed in policy, it is important that the stakeholders do assess the amorphous considerations.

Regularizing Artificial Intelligence Ethics in the Indo-Pacific, GLA-TR-002 (2021)

- Multilateralism could be considered as a "moral" approach to negotiate and design recommendations. However, multilateralism for AI ethics could be considered as a top-down mechanism, which again, in spirit might be agreed, but not in practice. Then, there are questions of regulatory competence and leverage, which governments would ask, thereby propelling for more plurilateral approaches to negotiate further.
- Indigenization, Localization and Economic Rights (ILER) would matter a lot in shaping each step of AI-related manufacturing to the stage of AI- based knowledge management in the Indo-Pacific region. A step by step approach can be dealt wherein the manifest availability of artificial intelligence can be closely looked into, and regional and local consensuses can be developed slyly. For example, in AI education, an estimate could be made as to in what respects the AI is subject to consideration, either as a Subject, an Object or a Third Party (SOTP Classification) [...] since either of the entitative classifications if are applied, the government authorities can audit the economic impact, and then, avenues of cooperation can be built. The economic aspects of RCA therefore must be taken into point.
- Any human-centric approach (HCA) to AI, cannot be unrealistic. Further, the HCA must not be in conflict with the RCAs adopted, which can be reasonably agreed by the Indo-Pacific. HCAs also should not limit the scope of review and decision- making to a rights-based approach (RiCA) where the exertion would be invested into merely creating

an infrastructure of rights enforcement without any weight. Instead, the centrality of human beings can be understood by the risks of algorithmic anthropomorphism, which compel governments to adopt quicker and permeable & interventionist RCAs. Hence, the focus of sensitivity must be not at investing at weightless or incoherent RiCAs, which have no virtual relevance to the strategic and risk considerations per se. A simple formation of any approach can be adopted by the governments in any of the following ways, non-exhaustively:

  - RiCAs must be central to the RCAs adopted, which then can shape the HCAs
  - HCAs can be based on the RCAs, which can then shape RiCAs
  - RCAs should be focusing on the element of anthropomorphism, a core component of HCAs, which can shape the RiCAs

- There will be a baggage of other risks, which may emerge in the fields, for example, environmental sciences, cybersecurity, telecommunication, commercial and economic law, and others. For each of them, HCAs, based on countering and understanding algorithmic anthropomorphism, can be very instrumental in shaping the RiCAs and RCAs comfortably.

- It would therefore become an interesting question whether there could be convergences on the RiCAs, RCAs and HCAs together in simultaneity. That is a contentious issue since there is no guarantee it can happen. The practicality and strategic relevance of any of the approaches would largely decide grounds to collaborate. RiCAs therefore need to converge to ensure that a comprehensive AI-related rights-based regulatory and foresight network can be established.

That can potentially happen when RCAs have larger scope of alignment, and the anthropomorphic element of HCAs becomes the optimal and larger quotient of risk (OLQR) realization. In such circumstances, RiCAs can be formidably adopted. Of course, the enforcement mechanisms would have limited aberrations, since RCAs are not the same anyways ideally. However, effective feedback in the form of jurisprudence, policy assertions and analyses can be put into good use.

- The case of the anthropological element of the HCAs becoming the optimal and larger quotient of risk is tricky, because it stems down to the R&D, skill and many other manufacturing and service sector compliance issues. How governments study and act robust is their business, but there even, a special focus should be on ILER. That would realistically shape the OLQR accordingly.

2021 Handbook on AI and International Law [RHB 2021 ISAIL] (2022)

Chapter 2

- In an example let's say that a person X in USA posts a social media post on a Canadian social media site which contains derogatory remarks against a person Y situated in Germany and the person X has social media friends list in 100 different countries. In such cases the public interest cannot be pinpointed to one singular location or a singular nation and the rights of access to justice of Y requires recognition of any judgment and their enforcement in those 100 different states for defamation issues. Such cases of social media cases cannot be even solved by exemplary costs granted in one nation because the standards of protection given to defamation varies from nation to nation.

- In such complex cases a practical approach of modular argumentation is suggested [...] which is a model suggested by Phan Minh Dung and Giovanni Sartor [...] which requires division of the case into various modules wherein each module prioritises a particular issue and in those concerned issues the relevant priority legal norm and the ensuing conflict is recognised and solved. However, a problem with such a model is the role of this modular segmentation that has to be done and by which court it is to be done. It is important to note that even the acceptance or denial of jurisdiction by a court (Government of India, 1908) is subjected to judicial review by courts of other nations before granting recognition to such form of modular argumentation. Further the applicability of such models becomes difficult due to the different approaches to the same rule of forum non conveniens recognised by various nations. For instance, in USA, the public and private interests both are recognised and considered (Blair, 1929; US Supreme Court, 1947), while in UK a greater preference is given to the overarching private and joint interests rather than public interests (House of Lords of the United Kingdom, 1987). Such differing approaches often lead to a difficulty in execution of this model of study.
- The problem would be further complicated where AI tools and algorithms automatically generate media and content in the Big Data cyberspace, wherein even nationality or domicile cannot be located or even the claimant's choice of jurisdiction becomes difficult to choose. While the problems are varied, but in commercial transactions involving AI, often the answer lies in Bilateral Investment Treaties referring such issues by default to arbitration and negotiation. But when it involves personal rights issues, crimes and civil acts often the most important consideration should be the point of enforcement and regulation. A concept of ISP Regulation developed by Russia (Wright,

2019) where the ISPs are made the central point of regulation and adjudication. The benefit of such regulation is that even though a jurisdiction is not existent but still the ISPs located in different nations can act as a filtering agency of data which can also impose stay proceedings or restoration proceedings to retract the data from the local networks. Therefore, the ISP which is responsible for propagation of the alleged data can be the locating factor for jurisdiction considering private and public interests concerned.

- In the regime of AI, the question of applicable law becomes complicated when AI driven technologies and automated technologies perform acts which become liable to civil or criminal acts. In this case not only the nationality or place of origin cannot be determined because of the AI being in the cyberspace but also because the laws which are to be applicable often conflict with each other. This question is suggested to be solved by the concept of contextual legal system.

Chapter 3

- Any of the obstacles to implementing AI include developing an AI approach with specific advantages, identifying individuals with matching expertise, facing a range of challenges faced by end-to-end rollout, and leaders' lack of interest and ownership in AI. Finance, telecom, retail, healthcare, and media all have strong penetration rates, indicating a fusion of incentives and engagement. In these industries, AI provides extensive value generation capability. Members of the sector are often open to engaging with AI. The use of AI software technology for data interaction and learning is highest in the Asia/Pacific financial market.

Chapter 4

- The issues with AI and economics are not just limited to its application in economics but also extends to its application in the economy itself. The application of AI in economics has also come with the advent of novel trends such as next level information asymmetries (Parks and Wellman, 2015). In agency theory it is widely recognized that agents do not always act in the best interest of their principal (Eisenhardt 1989). This is possible as and when agents have more information about a situation than their principal. The principal–agent problem arises, if the interest of the agent and the principal are not aligned and the agent exploits an existing information asymmetry (Parks and Wellman, 2015). Firstly, it's imperative to note that instead of just two actors there'll be three actors in a principal-agent relationship: the human user of AI as a principal, the AI agent, and the provider of the AI agent who is in a dual role. the AI provider owns the AI agent and is thus also in the role of a principal. On the other hand, the AI provider is a supplier of AI services to the user and thus in the role of an agent.

- Given that AI is a general-purpose technology, AI providers operate in multiple business environments and thus combine data collected and processed by a multitude of software agents in various domains like consumer behaviour, social media activities, or mobility.

Chapter 5

- The table above [in the chapter] showcases that artificial intelligence technologies used in global insolvency and bankruptcy processes include machine learning, deep learning, artificial neural networks, rules based expert systems and natural language processing. These artificial intelligence technologies have been often combined with

allied fourth industrial revolution technologies such as big data analytics and fuzzy matching. Unfortunately, no domestic or international legal instrument or policy instrument exists which stipulates rules or even remote guidelines in any manner for insolvency and bankruptcy processes. This is because artificial intelligence technologies have been underapplied in insolvency and bankruptcy processes.

Chapter 6

- Artificial intelligence technologies have been enabling taxation outcomes in calculation of tax liabilities, customs processes, tax compliance and tax enforcement activities. The inception of such usage began in 2008 and has been advancing rapidly ever since. The usage has been seen more by the private sector and unfortunately, Governments have been slow to adopt such technologies for enhancing tax enforcement and procedures within their own countries. It is noteworthy that the above assertion is only true for artificial intelligence applications in direct and indirect taxes which are imposed on income of individuals, businesses and other juridical persons. However, when it comes to customs duties, the exact opposite can be seen since the deployment of artificial intelligence technologies in customs procedures is a widespread phenomenon by several Governments and the involvement of the private sector is scarce.

Chapter 7

- Although a specific international legal instrument which is binding in force has not been witnessed in the global securities market for the regulation of artificial intelligence technologies, significant efforts have been seen from the International Organisation of Securities Commission. This is evident from the fact that the International Organisation of

Securities Commission has published guidance for intermediaries and asset managers using artificial intelligence and Machine Learning.

Chapter 8

- There have been manifold uses of artificial intelligence technologies in the sphere of litigation. However, no domestic law or international legal instrument exists in place which can regulate or at least prescribing guidelines at a bare minimum for the usage of artificial intelligence in global litigation practices. The use of artificial intelligence in alternative dispute resolution methods such as conciliation, mediation and arbitration have been considerably less compared to negotiation mainly because most jurisdictions and regional legal instruments require arbitrators, mediators and conciliators to be natural persons.

Chapter 9

- The table above showcases that artificial intelligence technologies being used in the global banking sectors are machine learning, supervised learning natural language processing, image recognition, text recognition, artificial neural networks, speech recognition, object recognition, facial recognition and computer vision which are coupled with non- artificial intelligence fourth industrial revolution technologies such as big data analytics and cloud computing. In some use cases, a combination of artificial intelligence software and hardware can be seen where the uses of robots, cameras and Automated Teller Machines have been seen. As per the table above, it is manifestly clear that the artificial intelligence technologies being used in the global insurance sectors are machine learning, deep learning, artificial neural networks, computer vision, facial recognition, image recognition, object recognition, natural

language processing, text recognition, speech recognition which have been combined with non- artificial intelligence technologies such as big data analytics and robotic process automation. In some use cases a combination of artificial intelligence software and hardware has also been seen with the help of cameras and smartphones.

Chapter 10

- It is unquestionable that advanced and AI-based technologies differ profoundly among one another on many grounds, first and most common of which is technicality. [...] There is no similarity between an expert system used in medical diagnosis, and an electronic toothbrush, or a collaborative industrial robot and a health- app, or a facial-recognitions system and a smart-thermostat, or a driverless vehicle and a chatbot, to name a few. Yet, all such applications would fall under the broad umbrella term of AI-based applications.
- It seems unavoidable and yet intermediation must consist in the adoption of specific solutions that consider relevant specificities which is not merely technical but also dependent upon factors like - the use made, the fundamental rights it impacts upon or contributes to satisfy, the nature of the party using and benefitting from it, the size of the potential market, and the clear identification of potential market failures, connected to the potential availability of adequate insurance products. [...] In such a perspective, all proposed solutions must be relevant and future proof and minimize legal uncertainty. It would certainly result in easing technological development and the flourishing of its connected industry and need to be technology specific.

- The technological evolution of the public sector is a gradual process that, for instance, saw the introduction of pen and paper as well as calculators and typewrites centuries ago. Non-learning algorithms have also been used in administrative processes for decades. Even computational learning has been used for quite some time, mainly in back-office operations such as in auto- correction tools for document management software or classification tools for online legislative databases. The capacity of these instruments to, at least in some circumstances, replace human decision-making processes has started to generate a debate about the desirability of their use. Beyond, administrations face pressure to adopt these instruments as the increased reliance on AI by the private sector 'demands that government agencies keep pace and make use of the same analytic tools to regulate the private sector more effectively'.

Regulatory Sandboxes for Artificial Intelligence: Techno-Legal Approaches for India, ISAIL-TR-002 (2022)

- Considering the fact that the sectors which have shown immense potential in artificial adoption in India have been discussed and the problems existing in current regulatory sandbox frameworks have also been discussed, it is necessary that certain viable recommendations are provided that attempt to create a legal structure for regulatory sandboxes for artificial intelligence technologies in India.
- So far, sectoral regulators have introduced regulatory sandboxes that are restricted to the respective sectors which operate completely within the limits of the powers

conferred to such sectoral regulators. Thus, in order to address the dilemma directly, the sector- wise approach will have to change to the technology- wise approach since the sector approach is much narrower than the technology- wise approach. This is because the idea and purpose of a regulatory sandbox is to promote innovation of a new technology rather than to promote sectoral development and by keeping a sector- wise approach, the core purpose of a regulatory sandbox is defeated. Emphasising on this, the shift of approach from sectoral to technological would mean that any legal framework proposed for regulatory sandboxes cannot be formulated through delegated legislation, as is being done currently and therefore, principal legislation will have to be framed. A principal legislation on regulatory sandboxes would harmonise various quintessentials of a regulatory sandbox, something which is not seen currently in the Indian scenario since sectoral regulators have continued to implement sandboxes as per the limitations and possibilities conferred to them through their respective enabling legislations.

- Moving forward, the proposed principal legislation would have to stipulate several provisions to achieve harmonisation amongst the necessities of implementing a regulatory sandbox. A provision for definitions will have to mandatorily be kept in order to avoid any ambiguities. This should, ideally be followed by the establishment of a statutory Innovation Office at the Centre and State Innovation Offices along with statutory authorities working in such Innovation Offices, that will assist in the designing, planning, implementation and solving field related problems during the operation of a regulatory sandbox. The qualifications, duties, powers and functions of the statutory Innovation Offices at the Centre and State levels and statutory authorities working in such Innovation Office will have to clearly be outlined.

- Considering the fact that a regulatory sandbox will never be limited to one form of technology, especially in the case of artificial intelligence since the utilisation of artificial intelligence is often seen with a combination of internet of things, big data analytics, cloud computing, blockchain and robotics, it is necessary that the principal legislation provides few mandatory provisions and confers liberty for specific regulations, rules, guidelines and frameworks to be made for particular forms of technology as and when regulatory sandboxes for such technological combinations are being implemented. This can be achieved by delegated legislation depending on the objective of the regulatory sandbox and the class of innovators being permitted to participate in the regulatory sandbox. Although eligibility and entry requirements can be prescribed by delegated legislation on the basis of the form of technology being proposed to be tested in the regulatory sandbox, it is necessary that the principal legislation itself provides standard provisions for duration of a regulatory sandbox. It is recommended that all regulatory sandboxes should be implemented and operated in cohorts for a standard period of 12 months (extendable for another period of 6 months only in cases of unforeseen exigencies) and the statutory Innovation Offices keep a check and report the progress of each and every cohort in the 12 months period. Standard provisions for exit from the regulatory sandbox will also have to be provided under this principal legislation. Needless to say, since several procedural portions of the regulatory sandbox will be governed by delegated legislation, the power to make rules, regulations, issue notifications and circulars will have to be conferred by the proposed principal legislation. Although having a minimum insurance requirement will not deter participation in the regulatory sandboxes, at the same time, it is pivotal to have provisions pertaining to incentives in the proposed principal legislation

on regulatory sandboxes. The incentives could involve several aspects such as the relaxation of licensing requirements in case suitable outcomes are achieved in the regulatory sandbox, concessions in the payment of electricity duties (a commodity required in insurmountable quantities while testing new technology) and a concessional rate of Goods and Services Tax for supplies made in relation to the testing of the new technology and permitted only during the period of participation of the innovator company during in the regulatory sandbox. In order to ensure that the incentives are utilised only towards the intended purpose, it is necessary that a Concession Agreement is entered between the statutory Innovation Office and the innovator company testing their product in the regulatory sandbox.

- Another indispensable set of provisions which the proposed principal legislation will have to deal with, is consumer protection and dispute resolution. In terms of consumer protection, apart from the minimum insurance requirement, a provision mandatorily requiring the innovator companies to take consent from consumers participating in the sandbox framework will have to be provided for along with reporting requirements to be complied by such innovator companies and supervised by the statutory Innovation Offices. Obtaining consent as prescribed by the proposed principal legislation will also help in ensuring that the liabilities of the innovator companies is not unlimited so as to deter them in testing their products effectively. However, there may arise several situations where the damage faced or the transaction entered into between the innovator company and the consumer participating in the sandbox framework are not as simple and therefore, it is necessary for the provisions of the proposed principal legislation to provide for a robust dispute resolution mechanism. It is recommended that a hybrid alternative dispute resolution method of mediation

followed by arbitration (commonly referred to as "Med-Arb") can be used for dispute resolution since the classes of disputes in a regulatory sandbox do not necessarily arise only between the innovator company and the consumer facing damage but also arise between two or more innovator companies participating in the regulatory sandbox framework and between the innovator company and the regulatory sandbox implementing authority. For this purpose, a panel of mediators and arbitrators can be formed as per rules and regulations prescribed in the delegated legislation and necessarily, experts in the fields of artificial intelligence and technology law can be appointed in the panel. This will not only help in achieving outcomes of disputes sooner but also help in ensuring that disputes are being handled by experts in the field of technology and artificial intelligence.

- Lastly, considering the fact that the proposed statutory Innovation Offices will have to work in collaboration with the various Ministries of the Central Government, State Government and also with sectoral regulators, an enabling provision allowing Innovation Offices to actively undertake inter- departmental co-operation can be stipulated as well.
- In spirit, the recommendations provided above attempt mainly at harmonisation but also aim towards a robust legal framework for enabling technological innovation for taking place. It follows that if statute- governed regulatory sandboxes are implemented in India, the immense unexplored potential of artificial intelligence technologies which only seem to have done well in few sectors can also progress and be applied in other sectors as well leading towards a more quicker yet guided technological innovation in the country.

Deciphering Artificial Intelligence Hype and its Legal-Economic Risks, VLiGTA-TR-001 (2022)

The Working Conditions to Determine Artificial Intelligence Hype

Some of the key aspects discussed in report are about the perpetuation of the hype cycles and their formalisation in the legal rubric for regulators. We have also focused with a soft law perception to address larger economic and technical issues and offered recommendations. Based on our research, we have formulated seven **working conditions to determine artificial intelligence hype**, which are based on a set of stages:

Stage 1: Influence or Generation Determination

- **An Artificial Intelligence hype cycle is perpetuated to influence or generate market perception in a real-time scenario such that a class of Artificial Intelligence technology as a product / service is used in a participatory or preparatory sense to influence or generate the hype cycle.**

Stage 2: Influencing or Generating Market Perceptions & Conditions

- **The hype cycle may be continuous or erratic, but the real-time impact on market perceptions which affect the market of the product / services involving Artificial Intelligence technologies, as estimated from a standardised / regulatory / judicial / statutory point of view.**
- **The hype cycle may directly or indirectly perpetuate the course of specific anti-competitive practices.**
- **Beyond the real-time impact on market perceptions, the consecutive effects of the real-time impact may distort a limited set of related markets, provided that the specific anti-competitive practices are furthered in a distinct pattern.**

Stage 3: Uninformed or Disinformed Markets

- **The features of the product / service subject to hype cycle are uninformed / disinformed to the market. It may be stated that misinforming the market may be construed as keeping the market just uninformed, except not in mutually exclusive cases.**

Stage 4: Misdirected Perceptions in the Information & Digital Economy

- **The hype cycle may be used to distract the information economy by converting the state of being uninformed or disinformed into misdirected perception. This means that the hype cycle about a product or service may not clarify certain specifics and may cause the public or market players to distract their focus towards ancillary considerations, to comfortably ignore the fact that they have being uninformed or disinformed.**

Stage 5: Estimation of the Hype Cycle through Risk Determination

- **In addition, even if preliminary clarifications or assessments are provided to the market, the lack of due diligence in determining the inexplicable features of the Artificial Intelligence technology in any form or means as a part of the product or service involves the assessment of the hype cycle with a risk-centric approach.**

Recommendations in this Report

1. Companies must make it clear to the regulatory bodies on the investment and ethical design of the products and services which involve narrow AI and high-intensive AI technologies.
2. Maintaining efficient knowledge management systems catering to IP issues is important. It is essential that the economic and ethical repercussions of the biproducts of

knowledge management are addressed carefully due to the case that many Artificial Intelligence technologies still would remain inexplicable due to reasons including ethical ambiguity.

3. If Artificial Intelligence technologies are included at any managerial level groups, departments and divisions, which also includes the board of directors for consultative, reliance or any other tangible cause, then regardless of their attribution to the knowledge management systems maintained by the company itself, including concerns on intellectual property, a risk-oriented practice of maintaining legitimate and viable transparency on issues around data protection & privacy and algorithmic activities & operations must be adopted. Regulators can adopt for self-regulatory directives or solutions. In case regulatory sandboxes are necessary to be used, there must be separate guidelines (since they are not products or services) for such kinds of technologies by virtue of their use case in the realm of corporate governance.

4. The transboundary flow of data, based on some commonalities of ethical and quality assessment, can be agreed amongst various countries subject to their data localisation and quality policies. When it comes to Artificial Intelligence technologies, to reduce or detect the impact and aftermath of Artificial Intelligence hype cycles – governments must negotiate on agreeing for an ethical free flow of data and by mapping certain algorithmic activities & operations which affect public welfare on a case-to-case basis.

5. We propose that the Working Conditions to Determine Artificial Intelligence Hype can be regarded in a consultative sense a framework to intermix competition policy and technology governance concerns, by various

stakeholders. We are open to consultation, feedback and alternate opinions.

6. We also propose that the Model Algorithmic Ethics Standards (MAES) to be put into use, so that some estimations, can be made at a preliminary level as regulatory sandboxes are subject to procurement.

Deciphering Regulative Methods for Generative AI, VLiGTA-TR-002 (2023)

Recommendations for Global Trends

- Develop clear regulations and frameworks to resolve intellectual property rights in generative AI. This includes determining the proprietorship of generated content, safeguarding original creations, and establishing licencing and usage guidelines.

- Implement stringent safeguards for data security and privacy protection. This includes assuring secure data handling practises, obtaining informed consent, anonymizing or pseudonymizing data as needed, and giving individuals control over their personal information. We have provided relevant suggestions in **Chapters 4 and 5**.

- Encourage AI systems to be transparent and explicable. Regulations should encourage the development of auditable and comprehensible AI models and algorithms in order to guarantee accountability and mitigate potential risks. We have provided relevant suggestions in **Chapters 4 and 5**.

- Artificial intelligence hype is a serious issue, and must be considered carefully, when dealt with. Mapping risk patterns

due to various generative AI tools, and their role in enabling misinformation or disinformation in their market practices, as discussed in **Chapters 4 and 5** must be considered.

- We urge that the classification methods we have developed in **Chapters 3 and 4**, i.e., the ontological categories could be used to develop industry classifications. We also are of the view that our suggestions on **Product-Service Classifications** can also be considered for implementation or legal purview at an initial level, as discussed in **Chapter 4**.

- Establish standard testing and certification procedures for generative AI systems to ensure their dependability, safety, and compliance with regulatory requirements. This may involve independent auditing, system behaviour verification, and adherence to specific quality standards. This should be similar to Standard Setting Organisations (SSO).

- The monopolistic nature of the generative AI industry, in terms of their use cases and their reliability / lack of reliability must be properly examined and assessed. Blueprinting and collection of relevant and credible trends would be important. We have provided relevant suggestions in **Chapters 4 and 5**.

- Countries in the Western Europe and North American region must take into account the concerns of the Global South countries including India, and not develop such standards and related legal expectations, which are designed to be rendered infructuous in application.

Recommendations on India's Digital Public Infrastructure

A New Artificial Intelligence Strategy for India [Proposal]

The main suggestion is to support the creation of a local generative AI engine that can be used to India's different Digital Public Infrastructures (DPIs). This suggestion intends to advance technological independence and self-reliance in the generative AI space. India can accomplish the following by creating a homegrown generative AI engine:

Technical independence: By developing a homegrown generative AI engine, India can reduce its reliance on proprietary systems and foreign technologies. Greater control and customization of AI tools is possible in accordance with the unique demands and specifications of DPIs.

Localization and Cultural Relevance: Creating a generative AI engine that is native to India gives researchers the chance to incorporate regional languages, cultural contexts, and a variety of datasets that are pertinent to the Indian context. As a result, the created content and AI apps are more accurate, sensitive to cultural differences, and tailored to Indian users' demands.

Data sovereignty: India can have more control over the data produced and processed by AI systems thanks to the development of a homegrown generative AI engine. This aids in addressing data sovereignty concerns and guarantees that private information is safeguarded in accordance with Indian privacy and data protection laws.

Economic Opportunities: Building a homegrown generative AI engine in India may result in the expansion of a thriving AI industry. For entrepreneurs, researchers, and technology businesses engaged in the creation and application of artificial intelligence, it can encourage innovation, draw investments, and open up economic opportunities.

A New Artificial Intelligence Strategy for India [Proposal]

Recommendations on India's Regulatory Infrastructure

Responsibility and Ethical Principles: Establish and uphold ethical principles for generative AI that take into account ideas like justice, transparency, responsibility, and human rights. Make sure that any ethical or legal transgressions by generative AI system developers, deployers, or users are held accountable by regulatory frameworks.

Regulatory Environment: Create regulatory sandboxes or controlled environments in which innovators and developers can experiment with generative AI technologies under the supervision of regulators. This provides the opportunity to test new concepts while assessing potential risks and developing appropriate regulations. We have provided relevant suggestions in **Chapters 4 and 5**.

AI-enabled Dispute Resolution: The emergence of AI-powered Online Dispute Resolution (ODR) platforms has revolutionised the dispute resolution landscape. These platforms have made dispute resolution more convenient and accessible, thereby reducing the need for in-person hearings. The integration of AI technology can facilitated online dispute resolution practices, making it a more efficient and effective process **leading to a stable dispute prevention and resolution environment. Regulators must be careful in assigning relevant use cases, as we have discussed in Chapters 3 and 4 in the sections related to Artificial Intelligence Hype and Product-Service Classifications.**

Promoting Economy of Innovation through Explainable AI, VLiGTA-TR-003 (2023)

Recommendations in this Report

Converging Legal and Business Concerns

- Legal and Business concerns can be jointly addressed by XAI where data collected from XAI can be used to address the regulatory challenges and help in innovation, while ensuring accountability on the forefront.
- Additionally, information from XAI systems can assist in developing and improving specific tailor made risk management strategies and ensure risk intervention at the earliest.
- Explainable AI tools can rely on prototype models which will have self-learning approaches to adopt and learn model-agnostic explanations is also highly flexible since it can only access the model's output.
- Privacy-aware machine learning tools can also be incorporated into the development of explainable AI tools to avoid possible risks of data breaches and privacy. Compliances may be developed and used for development purposes, including the general mandates that are attributed to them.

Conflict Management

- Compliance by design may become a significant aspect of encouraging the use of regulatory sandboxes and enabling innovation management in more productive ways as possible. In case sandboxes are rendered ineffective, real-time awareness and consumer education must be done, keeping in mind technology products and services accessible and human-centric by design.
- Risk Management strategies are advised to be incorporated at different stages of AI life cycle from the inception of Data collection and Data training.
- De-risking AI can involve model risk assessment by classifying AI model based on its risk (High, low, medium) and its contextual usage which will further assist in developers, stakeholders to jointly develop risk mitigation principles according to the level of risk incurred by AI.

- Deployment of AI explainability measures will require a level of decentralisation where transdisciplinary teams to work closely to provide complete oversight. Risk monitoring should be carried out by data scientists, developers and KMPs to share overlapping information and improve situational analysis of the AI system periodically.

Innovation Management

- The element of trust is necessary and the workflow behind the purpose of data use must be made clear by companies.
- Even if the legal risks are not foreseeable, they can at least make decisions, which de-risk the algorithmic exploitation of personal & non-personal data, metadata and other classes of data & information.
- These involve technical and economic choices first, which is why unless regulators come up with straightforward regulatory solutions, companies must see how they can minimise the chances of exploitation and enhance the quality of their deliverables and keeping their knowledge management practices much safer.