# A NEW HORIZON FOR AI REGULATIONS

Kanya Rai*

**Abstract**

The World Trade Organization (WTO) plays a pivotal role in governing and facilitating global trade, with its foundation rooted in principles such as non-discrimination, reciprocity, transparency, and safety valves to protect domestic industries. Established on January 1, 1995, as the successor to the General Agreement on Tariffs and Trade (GATT), the WTO oversees a comprehensive framework of agreements that regulate various aspects of international commerce. These include the General Agreement on Tariffs and Trade (GATT), General Agreement on Trade in Services (GATS), Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), and several others that collectively aim to promote free and fair trade. Central to the WTO's mandate is its dispute resolution mechanism, which provides a structured process for addressing and resolving trade conflicts among member nations. This mechanism involves stages of consultation, panel proceedings, appellate review, implementation, and compliance surveillance. The effectiveness of this system has reinforced the rule of law in international trade, contributing to a more stable and predictable trading environment. WTO regulations have significantly impacted global trade by promoting trade liberalization, enhancing market stability, and facilitating economic growth through increased efficiency and productivity. However, the organization also faces challenges and criticisms, such as perceived inefficiencies in decision-making, biases favoring developed countries, and occasional enforcement difficulties. This comprehensive exploration examines the core principles and agreements that underpin the WTO, delving into its regulatory framework and the mechanisms employed for dispute resolution. It assesses the impact of WTO regulations on global trade and discusses the ongoing challenges faced by the organization. Through this analysis, the essential role of the WTO in fostering a fair and inclusive global trading system is highlighted, while also recognizing the need for continual adaptation and reform in response to the dynamic nature of international trade.

* Author

## INTRODUCTION

Artificial intelligence (AI) is the science and technology that allows computers and other digital devices to read, write, analyze, learn, and create. It is the ability to make robots think like humans and make decisions.

The adoption of AI is outpacing the creation of legislation and regulations pertaining to it.

While technology offers nations all around the world enormous opportunities, there are also possible risks. The headlines of today tend to hint at recommendations for AI rules to legislators, and it is hardly surprising that the majority of nations have adopted regulations pertaining to AI that are remarkably similar. By drawing large amounts of foreign direct investment, India expands its basis for a high-tech labor force and dives into becoming a significant player in the global technology chain. AI-driven technology is developing as a result of this expansion across a number of Indian economic areas, including the labor, education, healthcare, and technology sectors. India does not yet have a formal legal framework for artificial intelligence (AI), but through its premier public policy think tank, NITI Aayog, the Indian government has brought attention to a number of advisories, regulations, and IT rules that provide a legal framework for the development of AI, generative AI, and large language models (LLM) in India.

On March 1, 2024, the Indian government released an advisory telling platforms to wait to implement any "unreliable Artificial Intelligence (AI) models/ Large Language Models (LLM)/ Generative AI, software or algorithms" until they have received explicit permission from the Ministry of Electronic Information Technology (Meit Y). Additionally, the intermediaries or platforms must make sure that their systems do not support discriminatory, biased, or undermine the integrity of the electoral process. Finally, they must label all artificially generated media and text with unique identifiers or metadata to make identification easier. Subsequently, Rajeev Chandrasekhar, the Minister of State for Electronics and Information Technology, clarified on platform X, Twitter, that the advisory was only intended for untested AI platforms that have been deployed on the Indian internet and that it was only applicable to "significant platforms" and that only "large platforms" are required to request permission from MeitY, not all startups. The government did, however, have to release an amended advice eliminating the requirement for platforms to submit action taken-cum-status updates in response to strong public criticism while maintaining the immediate compliance requirements. To alert users to potential errors, two labels were introduced: under-tested or unreliable AI models. The platforms were required to self-identify under these labels. The idea of the "first originator" was dropped. The introduction of consent pop-ups aimed to clearly alert users to the untrustworthiness of content generated by artificial intelligence.

The following are important tactics and principles to consider while creating and utilizing AI technology in a responsible manner to influence India's regulatory environment:

## 1. The first national AI strategy, NATIONAL ARTIFICIAL INTELLIGENCE STRATEGY

#AIFORALL, was unveiled by Niti Ayog in 2018 to establish national priorities for innovation and deployment in a number of industries, including healthcare, education, smart mobility, smart cities and infrastructure, transformation, transportation, and agriculture. High-quality dataset generation to support research, innovation, and the development of legislative frameworks to safeguard data and cybersecurity will follow the introduction of this plan.

## 2. RESPONSIBLE AI PRINCIPLES

In February 2021, NITI Ayog, in the midst of implementing the National Artificial Intelligence Strategy, drafted the Principles for Responsible AI, which explores ethical issues surrounding the application of AI solutions in India. System Consideration explores principles of decision-making, and the inclusion of beneficiaries through equitable means and accountability, and Societal Consideration explores the impact of automation on job creation and employment. Seven additional guidelines for the responsible implementation and governance of AI are defined in this draft:

A. Dependability and safety

B. Non-discrimination and inclusivity

C. Equality

D. Security and privacy

E. Transparency

F. Accountability

G. Preservation and upholding of human values.

## 3. PRINCIPLES OF OPERATIONAL-IZATION FOR RESPONSIBLE AI

August 2021 saw the publication by NITI Aayog of the second section of the principles for responsible AI, which looks at the operationalizing practices that come from ethical considerations. It also emphasizes the importance of government involvement in promoting responsible AI in social sectors while working with the private sector and research organizations, emphasizing the necessity of regulations and policy actions, capacity enhancement, and encouraging ethical practices by integrating a responsible mindset among private entities regarding AI. Finally, it crowns regulatory and policy interventions, incentivizes ethics by design, builds capacity, and creates compliance frameworks with pertinent AI standards.

## 4. DIGITAL PERSONAL DATA PROTECTION ACT (DPDP Act) enacted by the Indian

President on August 11, 2023, came into immediate force. The act addresses certain privacy concerns pertaining to AI platforms and focuses on the administration of digital personal data processing in India.

## 5. INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES

**AND DIGITAL MEDIA ETHICS CODE), 2021**

The Government of India issued IT Rule 2021, which was amended on April 6, 2023, and went into effect on May 26, 2021. It provides a framework for monitoring organizations such as over-the-top platforms, digital news media, and social media intermediaries.

## 6. WORKING POLICY FOR THE NATIONAL DATA GOVERNANCE FRAMEWORK

MeitY published the policy on May 26, 2022, with the goal of improving the government's data gathering and management procedures and offering a contemporary framework. By creating an extensive dataset repository, its main goal is to encourage data-driven research, businesses, and an ecosystem that is favorable to AI in India.

## 7. FRAME ESSENTIAL STANDARDS

The Ministry of Electronics and Information Technology and the Bureau of Indian Standards have established two committees tasked with reporting on the advancements in AI, safety and ethical issues, and developing Draft Indian Standards for responsible AI, respectively.

## 8. PROTECTION FROM DEEPER FAKES

Deepfakes are harmful activities that aim to disseminate false information using digitally altered photos, audio, and videos. Because of their hyper-realistic appearance, deepfakes have the potential to damage someone's reputation, tamper with evidence, and undermine trust in institutions.

Section 66E of the Information Technology Act, 2000 regulates deep fakes, which carry a maximum three-year jail sentence or a fine of INR 200,000. The IT Act's Sections 27, 27A, and 67B control the publication and transmission of offensive deepfakes. They also require the prompt removal of such content, risking social media sites' loss of "safe harbor" protection. Section 66D governs the use of computers and communication devices maliciously. Section 509, Section 499, and Section 153(a) and (b) of the Indian Penal Code regulate insulting modestly of a woman, criminal defamation, and promoting enmity on communal lines accordingly. The Copyright Act of 1957 forbids the unapproved use of copyrighted content to produce deepfakes (Section 51).

## AI INTERMEDIARIES' DUE DILIGE-NCE ADVISORY AND THE IMPLICATIONS OF NON-COMPLIANCE

On March 1, 2024, the prior advisory eNo.2(4)/2023-CyberLaws-3 was revised. On March 15, 2024, MeitY released a new advisory that raised concerns about platforms and intermediaries failing to exercise due diligence as required by IT Rules 2021.

1.Rule 3(1)(b) of the IT Rules, the IT Act 2000, or other applicable laws are examined in the advisory, and they state that intermediaries and platforms must make sure that users cannot host, display, upload, modify, publish, transmit, store, update, or

share any unlawful content through the use of AI models, LLM, Generative AI, software, or algorithms.

2. The election process's integrity should not be jeopardized by computer resources that use LLM, Generative AI, Software, or AI models to create bias or discrimination.

3. Indian users should only have access to software, algorithms, LLM, Generative AI, and under-tested or unstable AI models when the resulting output has been accurately labeled.

4. Text, visual, audio, and audio-visual information should be labeled or embedded with permanent unique metadata or identifiers to prevent misinformation or deepfakes that are made possible by intermediaries. This metadata should also allow the identification of the users or computer resources that made the changes.

5. Users should be made aware of the terms of service and user agreements on the handling of illegal material. This includes restricted access, suspicious accounts, terminations, and penalties under applicable laws.

6. Intermediaries, platforms, and their users risk prosecution under the IT Act 2000 and other criminal laws for failing to comply with the IT Rules and/or Act 2000.

Global Collaboration on Artificial Intelligence and Global Partnership

India participates actively in the GPAI. Experts in data governance, responsible AI, the future of work, innovation, and commercialization presented their deliverable work at the 2023 GPAI Summit in New Delhi. These topics can be incorporated into national plans of members to guarantee the equitable and sustainable growth of AI. The 2023 Ministerial Declaration was adopted by the members of the GPAI, reiterating their commitment to responsible and trustworthy AI supervision in accordance with the AI Principles of The Organization for Economic Cooperation and Development. They also committed to putting the suggested principles into practice by developing rules, policies, standards, and other initiatives, which will help to close the knowledge gap and advance sustainable, inclusive, and responsible AI.

General Atomics Aeronautical Systems, Inc. and 114ai, an AI company based in India, have partnered to develop cutting-edge technologies for intricate military systems.

The US-based semiconductor company NVIDIA Corporation announced a collaboration with TATA Group and Reliable Industries Ltd. to create language models and cloud infrastructure. NVIDIA will supply the processing capacity needed to create a cloud AI infrastructure platform.

In order to avoid future obstacles relating to liability for harm, rights to intellectual property for AI systems, privacy, and data protection, India is advised to develop the best legal framework and path to explore such international opportunities and strengthen the foundation of its AI expansion through joint ventures, strategic alliances, or wholly owned subsidiaries, depending on the level of investments and control required by the investing foreign entity.

Democracies face enormous problems from AI, which endangers people's rights, restricts

their options, and blocks them from accessing essential resources or services. Relevant instances of careless and extremely harmful AI can be found all over the world. For instance, in America, a system meant to care for patients was found to be unsafe, biased, and ineffective; unrestricted social media data collection has been used to threaten opportunities, disregard privacy concerns, and persuade people to track their activities without their knowledge or consent. However, who would have thought that computers meant to forecast storm patterns could also be used to apply algorithms to diagnose patients' illnesses, transforming entire industries? Artificial intelligence (AI) is developing into a potent instrument when used properly.

President Biden affirms that American innovation will power artificial intelligence (AI), which has the potential to redefine every aspect of our society and upskill lifestyles, but it will not come at the expense of civil rights, democratic values, or fundamental American principles. He refers to the right to privacy as "the basis for so many more rights that we have come to take for granted that are ingrained in the fabric of the country." Upon taking office, President Biden directed the federal government as a whole to eliminate racial injustice and inequality, promote fairness in decision-making procedures, and uphold equal opportunities and progressive civil rights. In response to these directives, the White House Office of Science and Technology Policy established five guiding principles for the development, use, and use of automated systems in the AI era that will safeguard the public in the United States. From Principles to Practice is a manual that was created with assistance from journalists, technologists, advocates, researchers, and policymakers. It is a framework with specific steps for putting protection policies and practices into practice during the technology design process. It helps people get experienced and well-rounded advice on AI systems that have the potential to significantly affect opportunities, civil rights, and access to necessities. The Blueprint for an AI Bill of Rights serves as a roadmap for a country looking to defend its people against threats posed by AI.

The White House Office of Science and Technology Policy has established five clear principles, which are as follows:

## SYSTEMS THAT ARE SAFE AND EFFECTIVE

In order to discover potential problematic hazards, AI technologies should be developed, deployed, and designed in consultation with a variety of communities, domain experts, and stakeholders. Additionally, one should be safeguarded against harmful or ineffective AI systems that jeopardize personal or public safety. In order to make sure AI systems are safe, effective, and compliant with domain-specific standards, pre-deployment testing and ongoing monitoring should be put in place. Based on how the systems are used, precautions should be taken to minimize any risks, and the findings should be made available to the public wherever feasible. Any data that is deemed unsuitable, harmful, or risky should be removed along with the system from use.

## 2. PROTECTIONS FROM ALGORITHMIC DISCRIMINATION

In order to proactively prevent unjust treatment and discrimination of people on the basis of race, ethnicity, sex, color, age, national origin, religion, genetic information, disability, veteran status, or any other classifications which are protected by law, system algorithms should be developed, deployed, and designed by developers, deployers, and designers. To verify these safeguards, if feasible, an impartial assessment and plain language reporting in the form of an algorithmic effect assessment, including the outcomes of disparity tests and mitigating data, should be carried out and made available to the public.

## 3. PRIVATE DATA

Because data privacy gives you control over how your information is used, it seems sense that built-in safeguards will shield you from unethical data activities. The AI system's architecture should respect privacy, the data collecting process should be legitimate and consistent with reasonable expectations, and the data collection should only be required in order to gather specified content. Users should be allowed to express concerns about the gathering, using, transferring, and erasing of data in suitable and meaningful ways, and their consent should be brief, clear, and written in plain English going forward. In the areas of employment, housing, and education, rights, opportunities, and access should not be hampered or limited by ongoing surveillance and monitoring. You should come first when it comes to enhanced protections and restrictions for data and inferences pertaining to sensitive domains like health, work, education, criminal justice, and finance, as well as for data about youth. These should only be used for necessary purposes to shield users from ethical review and use prohibitions.

## 4. NOTICE AND AN OUTLINE

The user ought to comprehend how and why the employment of an automated system results in outcomes that have an effect on them. The designers, developers, and deployers should provide a generally accessible, technically sound, meaningful, and plain language summary document that explains how the system functions overall and details role automation plans. It should also include a warning about using such systems, a list of everyone involved in the system, and a timely, clear, and accessible explanation of the results.

## 5. HUMAN REPLACEMENTS, THOUGHT, AND REVERSAL

When appropriate and considering reasonable expectations in a particular context, you should be able to opt out of the automated system, protect the public from particularly harmful effects, and have access to a person who can promptly address any issues you run into. When an automated system malfunctions or makes a mistake, consumers should have access to prompt, fair, efficient, maintained solutions along with suitable operator training and remedies that don't put undue stress on the general public. Public release of a report that describes human governance procedures and evaluates their efficacy, timeliness, accessibility, and results is required.

## USING THE BLUEPRINT TO APPLY A BILL OF RIGHTS FOR AI

This framework outlines the safeguards that ought to be put in place for any AI system that might have an effect on a person's ability to exercise their rights, access, or opportunities.

Regardless of how AI develops in our lives, the framework applies to AI systems that have the potential to significantly affect the rights of the American public and their equal and complete protection when it comes to essential resources, services, or opportunities.

Equal access to housing, loans, jobs, education, and other services are examples of equal opportunities. Financial services, social services, safety, healthcare, government benefits, and non-deceptive services regarding goods and services are among the essential resources or services that are easily accessible. Voting, expression, protection against discrimination, illegal monitoring, harsh penalties, and other freedoms in both the public and private spheres are all considered civil rights, civil liberties, and privacy.

When taken as a whole, the Blueprint for an AI Bill of Rights' five guiding principles and related activities overlap in that they promote protectionism against possible harm from automated systems. As a result, when the entire overlapping framework is considered, that is, the protective measures implemented, the degree and kind of harm or risk to people's rights, opportunities, and access should be taken into account.

In order to prevent potential misuse or unintended consequences of artificial intelligence (AI) systems, the U.S. National Institute of Standards and Technology is hosting workshops and discussions with both the public and private sectors. Additionally, the institute is working to develop federal standards for the development of robust, trustworthy, and dependable AI systems. During the 2023 legislative session, over twenty-five states introduced legislation related to artificial intelligence (AI), and eighteen of those states passed resolutions or passed laws containing provisions such as the following: the Department of Administrative Services was mandated to conduct an inventory of all AI-enabled systems used by state agencies, and the Office of Policy and Management was required to establish policies and procedures regarding the development, implementation, procurement, utilization, and ongoing assessments of AI-enabled systems used by state agencies. An AI advisory committee was established by the states of Texas, North Dakota, Puerto Rico, and West Virginia to research and oversee AI systems that are used, produced, or purchased by state agencies. To help some small and medium-sized manufacturing businesses adopt new "Industry 4.0" technologies or associated infrastructure, Maryland developed the Industry 4.0 Technologies Grant Program.

### Act on Artificial Intelligence of the European Union

In order to provide improved conditions for the advancement and application of this cutting-edge technology, the European Union drafted the first complete set of regulations on artificial intelligence in history. The European Commission unveiled the first AI regulatory

framework in April 2021. This framework evaluates and categorizes AI systems according to the risk level that each one poses for various applications, and it applies varying degrees of rules in accordance with that classification.

Establishing a uniform and technologically neutral definition of artificial intelligence (AI) that could be applied to future AI systems, the parliament wants to ensure that AI systems used in the EU are transparent, traceable, safe, environmentally friendly, and non-discriminatory. It also instructs automation to not oversee AI systems in order to prevent harmful outcomes. High-risk systems had more time to comply with the requirements because the obligations pertaining to them were applicable 36 months after they entered into force, with the exception of some that were applicable sooner. The AI Act was adopted by the Parliament in March 2024 and became fully applicable 24 months after it entered into force.

- Rules on general-purpose AI systems that must adhere to transparency requirements will take effect 12 months after the entry into force.
- The prohibition on AI systems that pose unacceptable risks will take effect six months after the entry into force.
- Codes of practice will take effect nine months after the entry into force.

The AI Act creates new regulations that, based on the degree of risk from AI, impose obligations on providers and users:

**UNACCEPTABLE RISK**

AI systems that are deemed to be a threat to humans will be prohibited under this; however, there may be some exceptions made for law enforcement.

- Social scoring is the process of categorizing people according to their behavior, socioeconomic status, or personal traits. This can be applied to individuals or particularly vulnerable groups.
- The classification and biometric identification of individuals. Only a small number of serious cases will be permitted to use real-time remote identification technologies; serious offenses will only be prosecuted with court sanctions using post-remote biometric identification systems when identification takes place after a considerable amount of time.
- Biometric identity technologies that operate remotely and in real-time, such as facial recognition.

**A HIGH RISK**

Under this, AI systems will be split into two groups and deemed high risk due to their detrimental effects on people's safety or fundamental rights. People will have the ability to raise concerns against AI systems with specified national agencies, and these systems will be evaluated both before and during their lifecycles before being placed on the market.

1. AI systems utilized in goods covered by EU product safety laws, such as toys, vehicles, elevators, airplanes, and medical equipment.

2. The following AI systems that fit into particular categories will have to register with the EU database:

- Education and career training;
- Critical infrastructure management and operation;
- Access to the use of public and private services and benefits;
- Employment, worker management, and self-employment;
- Law enforcement;
- Management of immigration, asylum, and border controls;
- Help with legal interpretation and application.

## PRESENTATION REQUIREMENTS

While some systems—like ChatGPT and Generative AI—won't be regarded as high risk, they will be forced to abide by EU copyright rules and transparency standards. Certain all-purpose AI models, such as GPT-4, which have a significant influence and may present systemic risk, must undergo assessments, and any significant occurrences must be notified to the European Commission. In order to alert consumers when they encounter such contents, images, audio files, or video files that are created or altered by AI systems must be properly labeled as such.

The following are the obligations:

- Declaring that the content was produced by AI
- Creating a model that stops it from producing stuff that isn't authorized
- Disseminating condensed versions of training-related copyrighted data

## AIDING WITH INNOVATION

The national authorities are expected to provide enterprises with a testing environment to imitate situations near to the actual world. This allows small and medium-sized businesses and startups to create and train AI models before making them available to the wider public.

In 2021 and 2022, China became the first nation to develop and enforce legally binding guidelines and regulations on a few AI applications. These guidelines and regulations later served as the cornerstone of China's AI governance system. Political leaders in the United States alert the world about China paving the way for AI governance, but in order for the United States to challenge China for leadership in this area, it must first study China's AI laws and policy-making procedures. The major players in China's AI regulation have not been the president, Xi Jinping, or the leaders of the CCP (Cyber Administration of China). Rather, the major players are the outcome of a dynamic and iterative policymaking process that has been influenced by a variety of factors pertaining to both inside and outside the Chinese party-state, including mid-level bureaucrats, academics, technologists, journalists, and policy researchers at platform tech companies. Chinese academics, journalists, businesses, and state-run media outlets actively steered the country's AI debates on regulations by analyzing, adopting, and adapting ideas from the United States and other countries. This demonstrated

that Chinese regulators are open to learning from and modifying ideas from other countries, regardless of whether they originate from friends or enemies of the country.

1. The process began when the Chinese Communist Party (CCP) and the Chinese government-imposed regulations on recommendation algorithms, which are used to power everything from social media and navigation apps to e-commerce platforms. These regulations gave users the right to be recommended content, protected gig workers, and required businesses to get involved in content recommendation.

In order to ensure that promoted content adheres to "mainstream value orientation," recommendation algorithm service providers should establish a mechanism for manual intervention in "top searches" rather than "hot topics," and they should be able to "actively transmit positive energy" while avoiding "disrupting economic and social order." Companies are required to uphold the rights of workers whose schedules are determined by algorithms to just compensation and sufficient rest, refrain from engaging in "unreasonable" price discrimination based on user characteristics, and refrain from using algorithms for monopolistic or unfair business activities. The primary rights of users include the ability to disable algorithmic suggestions for a particular app or website, to choose or remove particular user tags for personalized content recommendations, and to request an explanation if an algorithm materially affects their rights.

2. The usage of artificial intelligence (AI)-generated synthetic media, such as deepfakes, was subject to the second rule. Here, the AI providers must watermark AI-generated material to ensure that it respects people's "likeness rights" and doesn't damage the "image of the nation."

"Respect social mores and ethics" and "Adhere to the correct political directions, public opinion orientation, and value trends" were the overarching ideologies that underpinned the regulation of deep synthesis. The restrictions included not creating, disseminating, or publishing "fake news," reviewing deep synthesis prompts and outputs manually or through technology, reminding users to get permission before editing biometric features, conducting internal or external security assessments before editing biometric features, and creating content that "might involve national security" or "the nation's image." It will be mandatory for the service providers to do security evaluations and update the algorithm registry.

## HOW DID CHINA FORMED AI REGULATORY RULES AND SPECIFICATIONS?

The very first strategy used by China is “reverse engineering Chinese AI governance” that is, the analysis of the tool begins with the final product, they are broken down into components parts and are then traced backward using the “policy funnel”, the four layered China’s AI regulation that is Real World Roots (China’s macro-level economics, politics, social, and technological

environment which create the need for new policy, alongside limiting the options for regulations), Xi Jinping and CCP Ideology (the political and intellectual filters through which policymakers understand the issues), “world of ideas” (composed of the policy and academic debates that generate new policy proposals, as well as the corporate lobbying that attempts to steer or water down these proposals. These public discussions contribute to the CCP and Government Bureaucracy (which consists of the important ministries and CCP committees that create and finalize regulations), even though they do not entirely dictate policy.

Following Xi's legacy of "common prosperity," or the pledge to close the wealth gap, SAMR, China's top antitrust authority and co-signatory of the final version, took a number of anti-monopoly and unfair competition actions against China's top platform companies in 2020–2022, in accordance with the Anti-Monopoly Law and Anti-unfair Competition Law. A clause that created an additional obstacle to the use of algorithms for monopolistic or unfair competition was introduced. In order to protect workers' rights and interests, Article 20 was added, with a particular emphasis on workers' rights. It requires algorithm providers that offer "work dispatch services" to take into account workers' legal rights to compensation and rest, as well as to improve the algorithms that are used to assign orders or set worker salaries and schedules.

Within ten working days of being live, providers whose algorithms possess "public opinion properties or capacity for social mobilization" are required to establish an algorithm register.

The world was shocked by OpenAI's remarkable writings on a wide range of subjects when the platform, ChatGPT, was released five days after the deep synthesis regulation was signed.

Although the term "technologies for generating or editing text content" implied that ChatGPT would be subject to regulation, the Chinese government and CCP were unprepared for the impact and ubiquity of this new breed of large language models.

The goal of the Pan-Canadian Artificial Intelligence Strategy is to guarantee that AI operations are carried out in accordance with the highest ethical standards, with an emphasis on openness, equity, and privacy when using this technology in human-centered ways.

Japan released the Social Principle of Human-Centric AI in 2019. It focuses on a framework for AI that enhances lives while upholding human dignity, valuing diversity, and guaranteeing sustainability. The seven guidelines state that AI should protect privacy and not be used against people, that people should understand AI and how it works, that it shouldn't give unfair advantages to businesses, that it should be fair, transparent, and explainable in its actions, and that it should pave the way for new discoveries and technological advancements.

Japan adopted a two-pronged approach to regulation: Regulation on AI and Regulation for AI. The former aims to mitigate the risks associated with AI, while the latter modifies

laws in response to opportunities and expectations for the technology's expansion.

There are currently a lot of discussions over if, when, and how to regulate artificial intelligence (AI). For instance, the US AI Risk Management Framework and the EU's draft AI Act both use a risk-weighted approach, but the US framework includes nonbinding activities while the EU's plan includes directly binding legislation. In this manner, the nations may go in the same direction while taking different routes. The creation and regulation of AI is fraught with issues. For example, who should have judicial authority over AI governance? How is society meant to balance the conflicting demands of safety and innovation? What part does the government play in AI advancements? How should rules be modified for rapidly advancing AI technologies? How should a nation cooperate internationally to explore this new frontier while considering the incentives of its own interests? And a ton more. Every nation wants a taste of AI in this case, but they also want it prepared to their preferences. A lot of nations are focusing on the highest-risk applications of AI, such as facial recognition software or autonomous weaponry, and employing regulatory sandboxes to establish secure environments for AI exploration and innovation.

Artificial intelligence has been developed, adapted, and regulated through international initiatives. Transparency, accountability, and security are among the OECD's AI principles. The organization has created a set of guidelines to support AI that is reliable, creative, and considerate of democratic and human rights. The G20 AI Principles emphasize justice and human-centered values, which are in accordance with the OECD recommendations. A global AI regulatory framework is possible, but there are a number of obstacles in the way. For example, reaching consensus on such a framework would be challenging if different nations have different priorities and concerns regarding AI regulations. Some nations may view it as ceding their national authority over AI regulations. Moreover, the complexity and constantly changing nature of AI technology makes it challenging to create comprehensive regulations.

Even as we draw to a close with this document, it is important to acknowledge the ongoing advancements in artificial intelligence (AI) across societal, intellectual, legislative, industrial, and technological domains. Given the critical nature of artificial intelligence and the need to address the threats it poses to society, ethics, morality, privacy, accountability, and transparency, it is noteworthy that developing a comprehensive regulatory framework for AI may require establishing clear guidelines for each emerging aspect, enforcing fair distribution of its benefits, and enlisting the public, industry leaders, and governments in concert.