THE NATIONAL UNIVERSITY OF ADVANCED LEGAL STUDIES, KOCHI

DISSERTATION ON

TOPIC: **THE NEED FOR A GLOBAL REGULATORY FRAMEWORK FOR ARTIFICIAL INTELLIGENCE: IMPLICATIONS OF THE EUROPEAN UNION'S ARTIFICIAL INTELLIGENCE ACT 2024**

Submitted in partial fulfilment of the requirement for the award of the Degree of Masters in Laws (2023-2024)

In

INTERNATIONAL TRADE LAW

Submitted by

NAVANEETH. M

Reg. No: LM 0223017

Under the Guidance of

Dr. Athira P.S

CERTIFICATE

This is to certify that **Mr. NAVANEETH. M, Reg. No. LM 0223017** has submitted his Dissertation titled "**THE NEED FOR A GLOBAL REGULATORY FRAMEWORK FOR ARTIFICIAL INTELLIGENCE: IMPLICATIONS OF THE EUROPEAN UNION'S ARTIFICIAL INTELLIGENCE ACT 2024**", in partial fulfilment of the requirement for the award of Degree of Master of Laws in International Trade Law to the National University of Advanced Legal Studies, Kochi under my guidance and supervision. It is also affirmed that the Dissertation submitted by him in original, bona-fide and genuine.

Date: 21.06.2024
Place: Kochi

Dr. ATHIRA P.S
NUALS, Kochi

CERTIFICATE ON PLAGIARISM CHECK

This is to certify that **Mr. NAVANEETH. M, Reg. No. LM 0223017** has submitted his Dissertation titled "**THE NEED FOR A GLOBAL REGULATORY FRAMEWORK FOR ARTIFICIAL INTELLIGENCE: IMPLICATIONS OF THE EUROPEAN UNION'S ARTIFICIAL INTELLIGENCE ACT 2024**", in partial fulfilment of the requirement for the award of Degree of Master of Laws in International Trade Law to the National University of Advanced Legal Studies, Kochi under my guidance and supervision and the same has been checked for plagiarism in Grammarly on 21.06.2024 at 01:48 pm and is found to be 7%.

Date: 21.06.2024
Place: Kochi

Dr. ATHIRA P.S
NUALS, Kochi

DECLARATION

I declare that this dissertation titled, "**THE NEED FOR A GLOBAL REGULATORY FRAMEWORK FOR ARTIFICIAL INTELLIGENCE: IMPLICATIONS OF THE EUROPEAN UNION'S ARTIFICIAL INTELLIGENCE ACT 2024**", researched and submitted by me to the National University of Advanced Legal Studies, Kochi in partial fulfilment of the requirement for the award of Degree of Master of Laws in International Trade Law, under the guidance and supervision of **Dr. ATHIRA P.S** is an original, bona-fide and legitimate work and it has been pursued for an academic interest. This work or any type thereof has not been submitted by me or anyone else for the award of another degree of either this University or any other University.

Date: 21.06.2024
Place: KOCHI

NAVANEETH. M
Reg.No: LM 0223017
LL.M, INTERNATIONAL TRADE LAW
NUALS, Kochi

ACKNOWLEDGEMENT

Working on this dissertation has been both challenging and equally interesting. This Thesis nevertheless, is the result of the pertinent efforts and contributions of many people around me.

First and foremost, I would like to express my profound gratitude to my supervisor, Dr. Athira PS, for her unwavering support and for allowing me the freedom to tackle challenging questions and explore new avenues of research. The invaluable and positively critical advice I received was instrumental in crystallizing my thoughts for this paper. Her guidance and expertise were instrumental in the successful completion of this research.

I am deeply grateful to Prof. (Dr.) Mini S. Thampi, Director, Centre for Post-Graduate Studies, for her continuous help and encouragement throughout this journey. My sincere thanks also go to the Vice-Chancellor, Hon'ble Justice (Retd.) S. Siri Jagan, and the entire faculty at NUALS for their consistent guidance and steadfast support.

I extend my heartfelt appreciation to the University Library staff for their timely assistance, which was crucial in carrying out this research work.

Lastly, I am profoundly thankful to my family and friends. Their constant love and support have been the backbone of this project, allowing me to pursue it with full spirit and enthusiasm.

PREFACE

This dissertation is made in partial fulfilment of the requirement for the award of Degree of Master of Laws in International Trade Law to the National University of Advanced Legal Studies, Kochi.

This dissertation primarily examines the intersection of Artificial Intelligence and international trade practices, a subject of significant global discourse. The definition and regulation of AI remain contentious topics, with many nations striving to establish clear guidelines. Some jurisdictions have successfully implemented sector-specific AI regulations, creating further challenges for other regions and industries. AI technologies are now integrated into numerous everyday processes, underscoring the urgent need for comprehensive and universally applicable regulations. While AI brings substantial advancements, it also introduces ethical, privacy, and employment concerns. To address these issues and navigate the evolving AI landscape, it is imperative to establish robust regulations that ensure responsible and accountable AI development and deployment.

This thesis explores the ethical, legal, and economic implications of AI-powered systems. It provides an in-depth analysis of the European Union's Artificial Intelligence Act of 2024, highlighting its key challenges and insights. Additionally, the dissertation proposes various factors to consider when formulating AI regulations, aiming to contribute to the development of a cohesive and effective regulatory framework for AI.

I would also like endlessly thank all the people who had immensely helped me in the completion of this dissertation. I would specially like to show gratitude to my guide and teacher Dr. Athira PS for his enormous encouragement, support and valuable input.

LIST OF ABBREVIATIONS

A.I.	ARTIFICIAL INTELLIGENCE
AAAI	ASSOCIATION FOR THE ADVANCEMENT OF ARTIFICIAL
AI ACT	ARTIFICIAL INTELLIGENCE ACT 2024
AI HLEG	HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE
AGI	ARTIFICIAL GENERAL INTELLIGENCE
AU	AFRICAN UNION
DABUS	DEVICE FOR THE AUTONOMOUS BOOTSTRAPPING OF UNIFIED SENTIENCE
E.U	EUROPEAN UNION
EC	EUROPEAN COMMISSION
EUROPA	EUROPEAN UNION WEBSITE
FCAI	FORUM FOR COOPERATION ON ARTIFICIAL INTELLIGENCE
GDPR	GENERAL DATA PROTECTION REGULATION
GPAI	GENERAL PURPOSE ARTIFICIAL INTELLIGENCE
ICO	INFORMATION COMMISSIONER'S OFFICE
IEC	INTERNATIONAL ELECTROTECHNICAL COMMITTEE
IEEE	INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS
IP	INTELLECTUAL PROPERTY
ISO	INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
IT	INFORMATION TECHNOLOGY
ITU	INTERNATIONAL TELECOMMUNICATION UNION
ML	MACHINE LEARNING
NDGFP	NATIONAL DATA GOVERNANCE FRAMEWORK POLICY
NLP	NATURAL LANGUAGE PROCESSING
OECD	ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

PIPEDA	THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT
S.C	SECURITY COUNCIL
UAE	UNITED ARAB EMIRITES
U.S	UNITED STATES
UC	UNIVERSITY OF CALIFORNIA
UN	UNITED NATIONS
UNESCO	UNITED NATIONS EDUCATIONAL, SOCIAL AND CULTURAL ORGANISATION
UNHRC	UNITED NATIONS HUMAN RIGHTS COUNCIL
UNICRI	UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE
WTO	WORLD TRADE ORGANISATION

TABLE OF CASES

1. Andersen v. Stability AI Ltd., No. 23-cv-00201-WHO (N.D. Cal. Oct. 30, 2023)
2. Delhi Vyapar Mahasangh v. Flipkart Internet Pvt. Ltd. and Amazon Seller Services, Case No. 40 of 2019, (Order Jan. 13, 2020)
3. Doe v. GitHub, Inc., No. 22-cv-06823-JST (N.D. Cal. Jan. 3, 2024)
4. Getty Images (US), Inc. v. Stability AI, Inc., No. 1:23-cv-00135 (D. Del.)
5. Glukhin v. Russia, App No. 11519/20, 4 July 2023 (ECHR)
6. Guo Bing v. Hangzhou Wildlife World Service Contract Dispute, Zhe Jiang 0111 Min Chu No. 6971 (2019)
7. Haghshenas v. Canada (Citizenship and Immigration), 2023 FC 464
8. Huskey v. State Farm Fire & Cas. Co., No. 22 C 7014 (N.D. Ill. Sep. 11, 2023)
9. Infopaq International A/S v. Danske Dagblades Forening, (2009)
10. J.L. v. Alphabet Inc., No. 3:23-cv-03440 (N.D. Cal. July 11, 2023)
11. James v. Amazon.com.ca, Inc., No. 2023 FC 166
12. Mobley v. Workday, Inc., No. 3:23-cv-00770 (N.D. Cal.)
13. Orpheus Medica v. Deep Biologics Inc., 2020 ONSC 4974
14. P.M. et al. v. OpenAI LP et al., No. 3:23-cv-03199 (N.D. Cal. Jun. 28, 2023)
15. Pierre Corbiau v. Administration des Contributions, 1993 ECR I-01277 (European Court)
16. Rupendra Kashyap v. Jiwan Publishing House Pvt. Ltd., 1996 38 DRJ 81 (Delhi)
17. Silverman v. OpenAI Inc. et al., No. 3:23-cv-03416 (N.D. Cal. July 7, 2023)
18. Stephen Thaler v. Comptroller-General of Patents, Designs and Trade Marks, [2023] UKSC 49
19. Walters v. OpenAI LLC, No. 23-A-04860-2 (GA. Super. Ct. Jun. 5, 2023)

CONTENTS

CHAPTER 1

INTRODUCTION

Technology has been a key factor in influencing global trade dynamics. Among the technological advancements, Artificial Intelligence stands out as the most promising one. Artificial Intelligence, or AI, is a machine's ability to perform the cognitive functions we usually associate with human minds. It allows computers and machines to simulate human intelligence and problem-solving tasks. The ideal characteristic of AI is its ability to rationalise and take action to achieve a specific goal. AI encompasses various subfields, including machine learning and deep learning, which allow systems to learn and adapt in novel ways from training data.[1]

The field of AI has made significant developments since its origin, evolving from the field of science fiction to disruptive technology that is transforming different spheres of life. The potential applications of AI are endless. Different forms of AI are now embedded in many everyday processes, including voice recognition in smartphones and associated gadgets; content moderation; facial recognition and biometric identification systems; virtual customer service chatbots; language translation services; exploration features within e-commerce platforms and digital content streaming services; credit scoring; diagnosis and monitoring in healthcare sectors; and the management of entire supply chain including warehouses, shipping, and logistics.[2] Thus, AI will bring immense opportunities to the future and will undoubtedly benefit global trade.

While AI offers significant advancements, it also raises ethical, privacy, and employment concerns. To tackle this and survive in the world of AI, proper regulations are to be introduced to ensure responsible and accountable AI development and deployment.

SCOPE OF THE STUDY

Living without technology has become unfeasible in this realm of science and technology. AI is gaining substantial momentum, and it is crucial to begin by understanding its fundamental concept. This field is in the process of growth and holds immense potential

[1] David Marr, AI: A Personal View, The Foundations of Artificial Intelligence 97, Derek Partridge and Yorick Wilks Edition (2006)

[2] Alexander Titus & Adam Russell, *The Promise and Peril of Artificial Intelligence -- Violet Teaming Offers a Balanced Path Forward* (2023)

to revolutionise human interaction. AI is impeded into the lifestyle of humans and it cannot be separated easily in the present scenario. Thus, everything and anything is connected with AI, and understanding the concept itself requires technical and expert knowledge in the particular field. Understanding AI in its wider sense is, hence, difficult. So, the scope of this research is limited to its applicability in the field of international trade.

The initial purpose of this study is to analyse the definition and significance of the term AI. Additionally, it examines the development and chronology of AI and tracks it to its current state. Subsequently, it analyses this novel technology's impact on international trade, specifically addressing the legal and ethical factors involved. In addition, it examines the current legal frameworks and regulations from a worldwide standpoint. These regulations are primarily implemented on an experimental basis, and there is a dearth of comprehensive legislation governing AI. The primary emphasis of the research is the analysis of the recently implemented Artificial Intelligence Act by the European Union. The Act's shortcomings and their worldwide ramifications are also meant to be examined.

The effect of such scattered and unclear regulations might hinder international trade itself. Hence, it is imperative to establish a comprehensive framework to govern AI. This work aims to recommend the foundation for a worldwide regulatory framework and also seeks to examine the responsible world entity for formulating such regulations.

RESEARCH OBJECTIVES

1. To understand the definition, concept and history of Artificial Intelligence in the current scenario.

2. To analyse the impact and utilisation of Artificial Intelligence in enhancing and transforming international trade practices.

3. To analyse and compare the regulatory measures implemented by various countries and international organisations worldwide

4. To comprehensively analyse the European Union's Artificial Intelligence Act 2024, focusing on its regulatory framework, implementation challenges, potential impacts on various sectors, and implications for innovation and ethical AI development.

5. To assess the potential Brussels Effect of the Artificial Intelligence Act 2024

6. To provide some foundational principles essential for inclusion in the development of a comprehensive global AI regulatory framework.

RESEARCH QUESTIONS

1. How have Artificial Intelligence technologies influenced and disrupted traditional practices within international trade?

2. How does the regulation of the European Union impact the global market, and will there be a Brussels Effect?

3. How essential is an international trade policy by the advent of Artificial Intelligence technologies?

HYPOTHESIS

A. AI holds significant importance in the contemporary world and has become indispensable across various domains. Furthermore, it encompasses legal and ethical challenges that require comprehensive consideration.

B. An appropriate regulatory framework for Artificial Intelligence must be established, featuring a clear definition of AI that fosters innovation. This framework should also include guidelines on AI attribution, as well as its design, distribution and operation.

C. The current regulations have numerous issues and gaps, leading to a lack of proper oversight in many areas. It is essential to address the safety, security measures, and liability of designers and manufacturers.

D. Along with the framework, a set of ethical practices and guidelines on Artificial Intelligence must be established. This involves creating robust regulations for AI, adhering to the highest practice standards, and organizing research activities to be carried out by the government and other societal sectors.

RESEARCH METHODOLOGY

The research method adopted is doctrinal legal research. This work attempts to assess the current legal framework, focusing on the examination of existing legal articles and doctrines in this field to comprehend the current structure. It includes both primary and secondary sources. Primary sources include International Agreements, Treaties, International Instruments, Legislation and case laws. Secondary sources include reports by National and

International agencies, multinational organisations, customary rules, newspaper reports, articles, books, principles and concepts.

CHAPTERIZATION

The first chapter deals with a general introduction to the study, which includes the scope of the study, research objectives, research problems, hypothesis and the methodology followed. This second chapter, titled Disruptive Influence of Artificial Intelligence on International Trade Practices, focuses on examining the impact of Artificial Intelligence on traditional trade practices and its legal and ethical challenges. It also traces the evolution and various definitions of artificial intelligence. The third chapter, titled Artificial Intelligence Regulatory Initiatives- A Global Perspective, analyses the jurisprudential aspect of artificial intelligence, existing legal frameworks, and the various domestic laws that deal with artificial intelligence in several jurisdictions. It also traces the regulatory initiatives by multinational international organisations. The next chapter, titled The European Union's Artificial Intelligence Act 2024- An Analysis, llamprovides a comprehensive analysis of the European Union's inaugural Artificial Intelligence Act, implemented in March of this year. It examines each provision of the Act, highlighting key insights and implications. The legislative framework is meticulously reviewed to offer an in-depth understanding of its components and impact.

Many jurisdictions have implemented various approaches to regulate artificial intelligence, each fraught with its own set of issues and gaps, complicating matters and sometimes inadvertently creating trade barriers. Many countries lack clear guidelines to develop comprehensive national regulations for Artificial Intelligence. The introduction of the European Union's Artificial Intelligence Act of 2024 has compelled many nations to align with these regulations. The fifth chapter titled Global Impact of the AI Act 2024 And the Need for an International AI Regulation, examines the deficiencies within the AI Act 2024 and its potential Brussels effect on global jurisdictions. Furthermore, it underscores the necessity for an international framework for Artificial Intelligence regulation and anticipates the challenges such an initiative may encounter. The concluding chapter analyses the components and factors to be taken into account while building a good regulatory framework for artificial intelligence. It concludes by presenting findings and recommendations aimed at shaping a cohesive global AI regulatory framework.

CHAPTER 2

AI'S DISRUPTIVE INFLUENCE ON INTERNATIONAL TRADE PRACTICES

INTRODUCTION

"Machine intelligence is the last invention that humanity will ever need to make."[3]

- Nick Bostrom

The field of AI has made significant developments since its origin, evolving from the field of science fiction to disruptive technology that is transforming different spheres of life. The potential applications of AI are endless. Different forms of AI are now embedded in many everyday processes, including voice recognition in smartphones and associated gadgets; content moderation; facial recognition and biometric identification systems; virtual customer service chatbots; language translation services; exploration features within e-commerce platforms and digital content streaming services; credit scoring; diagnosis and monitoring in healthcare sectors; and the management of entire supply chain including warehouses, shipping, and logistics.[4] Thus, AI will bring immense opportunities to the future and will undoubtedly benefit global trade.

In this chapter, we shall analyse the history and evolution of AI technology, the available definitions of Artificial Intelligence, the influence of AI in International Trade and the legal and ethical challenges arising from AI integration.

HISTORY AND EVOLUTION

Artificial Intelligence is a term that originated in the 1950s, but the concept has an ancient origin. So, to truly understand the history and evolution of AI, we need to dig into its ancient roots, where the crucial aspects and concepts initially emerged. Throughout history, various milestones have paved the way for the development of AI. In the 4th to 3rd centuries BC, Aristotle introduced syllogistic logic, an early deductive reasoning system that

[3] *Nick Bostrom,* Superintelligence *(2014), http://books.google.ie/books?id=7_H8AwAAQBAJ&printsec=frontcover&dq=Superintelligence:+Paths,+Dangers,+Strategies&hl=&cd=1&source=gbs_api.*

[4] Asif, M., Gouqing, Z, *Innovative application of artificial intelligence in a multi-dimensional communication research analysis: a critical review*, Discover Artificial Intellegence, 4, 37 (2024). https://doi.org/10.1007/s44163-024-00134-3

laid the foundation for logical thinking and reasoning—integral aspects of AI. In the 12th century, "Talking heads" devices were reportedly invented, contributing to early experiments in replicating human speech and interaction. The 14th century witnessed the invention of the printing press using "Movable type" technology, a significant advancement in information dissemination that played a role in the spread of knowledge crucial for AI development. Clocks, the first modern measuring devices, emerged in the 15th century, aiding scientific and technological progress, including developments in AI.[5] Clockmakers expanded their skills to create mechanical animals, such as Rabbi Loew's golem, showcasing early human fascination with lifelike entities.[6]

The 16th century saw René Descartes proposing the idea of animal bodies as complex machines, contributing to the notion of mechanising living beings. The 17th century featured key developments, including Blaise Pascal's creation of the first digital calculating machine, Thomas Hobbes' publication of "The Leviathan" with mechanical and combinatorial theories of thinking, and Gottfried Wilhelm Leibniz's improvement of Pascal's calculating machine. In the 18th century, Joseph-Marie Jacquard invented the first programmable device—the Jacquard loom—advancing automation and control. Mary Shelley's 1818 novel "Frankenstein" explored themes of artificial life and the consequences of creating sentient beings.[7]

Moving into the 20th century, Karel Čapek's play "RUR" (Rossum’s Universal Robots) in 1921 introduced the term "robot" to the English language, contributing to the popularisation of artificial beings. In 1943, Warren McCulloch and Walter Pitts laid the foundation for neural networks, a crucial component of modern AI, with their publication "A Logical Calculus of the Ideas Immanent in Nervous Activity."[8] Isaac Asimov's "Three Laws of Robotics" and Claude Shannon's chess analysis in 1950 contributed to ethical considerations and game-playing in AI. The Dartmouth Summer Research Project in 1956 marked AI's formal inception, and the term "artificial intelligence" was coined by John McCarthy. The 1960s faced an "AI winter" with a decline in research, but the 1970s brought the backpropagation algorithm for neural network training. The 1980s saw the rise of expert

[5] Tanya Roay, *The History and Evolution of Artificial Intelligence; AI’s Present and Future*, All Tech Magazine, (2023) https://alltechmagazine.com/the-evolution-of-ai/

[6] Delipetrev, Blagoj and Tsinaraki, Chrysi and Kostic, Uros, *Historical Evolution of Artificial Intelligence,* Publications Office of the European Union (2020)

[7] Ibid

[8] Jung Lee et al., *Editorial: Functional Microcircuits in the Brain and in Artificial Intelligent Systems,* Frontiers in Computational Neuroscience (2023)

systems and Japan's Fifth Generation Computer Project. Neural networks declined in the 1990s, and support vector machines gained popularity.[9]

In the 2000s, data science emerged, and progress in Natural Language Processing (NLP) has enabled computers to comprehend human language more effectively and respond in a more human-like manner. The 2010s witnessed the rise of deep neural networks, which developed Deep Learning, a subset of machine learning, achieving state-of-the-art results like breakthroughs in areas such as computer vision and speech recognition. In the late 2010s and early 2020s, AI became a part of everyday activities, from virtual personal assistants to self-driving cars. Models like GPT have made significant contributions to the AI industry in recent years. By the end of 2020, AI has experienced significant expansion in NLP, computer vision, and ML.[10] The emergence of virtual assistants such as Siri and Alexa have popularised AI, and its growing utilisation across diverse sectors like healthcare, finance, and retail has showcased its practical implementation in real-world scenarios. Altogether, the journey of AI reflects a continuous quest for understanding and replicating intelligent processes throughout history.[11]

DEFINITIONS

Intelligence can be defined as the ability to learn and perform suitable techniques to solve problems and achieve goals, appropriate to the context in an uncertain, ever-varying world. A fully pre-programmed factory robot is flexible, accurate, and consistent but not intelligent.[12] The scientific community lacks a universally accepted definition for artificial intelligence, and the term ‘AI’ is frequently employed as a comprehensive label for diverse computer applications utilising various techniques that demonstrate abilities commonly linked with human intelligence.[13] Artificial Intelligence is a multifaceted field, and defining it accurately poses a challenge due to its evolving nature and diverse applications. Various perspectives from scholars, organisations, and regulatory bodies contribute to the complex landscape of AI definitions.

[9] Tanya Roy, supra note 5, at 18

[10] Zhou Shao et al., *Tracing the evolution of AI in the past decade and forecasting the emerging trends*, Expert Systems with Applications, *209, (2022)*

[11] Anurag, A.S, *The Evolution of AI and Data Science*, *The Ethical Frontier of AI and Data Analysis,* edited by Rajeev Kumar, et al., Hershey, PA: IGI Global, 295-312, 2024.

[12] Professor Christopher Manning, *Stanford University Human-Centered Artificial Intelligence*, September 2020

[13] Defense Science Board, *Council of Europe, Feasibility Study, Ad Hoc Committee on Artificial Intelligence, CAHAI* (2020-23)

Artificial Intelligence, according to the emeritus Stanford Professor John McCarthy, who coined the term itself in 1955, is "the science and engineering of making intelligent machines."[14] In its broadest sense, AI has been described as "the study of the computations that make it possible to perceive, reason and act"[15]. George F Luger and William A Stubblefield have defined it as "the automation of Intelligent behaviour which is driven by a general study of intelligent agents both biological and artificial"[16]. However, in concrete terms, and in most applications, AI is defined as "non-human intelligence that is measured by its ability to replicate human mental skills, such as pattern recognition, understanding NLP, adaptive learning from experience, strategising, or reasoning about others."[17] A definition that is also upheld in the Summer Study on Autonomy by the US Defense Science Board, which describes AI as "the capability of computer systems to perform tasks that normally require human intelligence"[18].

One of the foundational definitions comes from the father of AI, Alan Turing, who proposed the Turing Test in 1950. According to Turing, a machine could be considered intelligent if it could exhibit human-like behaviour indistinguishable from that of a human being during interactions. While this test remains influential, contemporary definitions have expanded to encompass a broader range of capabilities.[19]

The Dartmouth Conference in 1956, considered the birthplace of AI, defined the field as the "study of making machines do things that would require intelligence if done by humans."[20] This early definition emphasised the mimicking of human intelligence, a theme that persists in many contemporary perspectives. During the 21st century, the influential AI researcher Stuart Russell and the late Nobel laureate economist Vernon Smith offered a more nuanced definition. They described AI as "the study of agents that receive percepts from the environment and perform actions," focusing on the fundamental interaction between an intelligent agent and its surroundings.[21]

[14] Stuart J. Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th ed. 2021)
[15] Patrick Henry Winston, Artificial Intelligence (3rd ed. 1992)
[16] George F. Luger & William A. Stubblefield, Defense Science Board, *Artificial Intelligence: Structures and Strategies for Complex Problem Solving* (6th ed. 2008).
[17] Stuart Russell, supra note 14, at 20
[18] Defense Science Board, *Report of the Defense Science Board Summer Study on Autonomy* (Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, June 2016).
[19] Alan Turing, *Computing Machinery and Intelligence*, 433-460 (1950)
[20] History of Data Science, Dartmouth Summer Research Project: The Birth of Artificial Intelligence, 2021
[21] Patrick Henry Winston, supra note 15, at 20

Organisations have also contributed to the ongoing discourse on AI definitions. The Institute of Electrical and Electronics Engineers (IEEE) defines AI as "the design, development, use, and application of computer systems to perform tasks that normally require human intelligence."[22] The World Economic Forum (WEF) takes a holistic approach, defining AI as "a range of technologies that enable machines to perform tasks that would require human intelligence."[23] Moreover, the National Institute of Standards and Technology (NIST) emphasises the learning aspect, defining AI as "the ability of a system to learn from data, improve performance, and make decisions with minimal human intervention".[24]

The European Union, in its Coordinated Plan on an AI regulation through the AI Act defines "Artificial Intelligence system" as "a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments."[25]

Technically, AI is machine-displayed intelligence that simulates human behaviour or thinking and can be trained to solve specific problems. AI is a combination of components like Machine Learning techniques, Deep Learning, Neural networks, Cognitive computing, Natural language processing (NLP) and Computer vision.

Machine Learning (ML) is the major component or subset of AI that focuses on the development of algorithms and statistical models that enable computers to improve their performance on a specific task over time without being explicitly programmed.[26] ML includes various approaches such as supervised learning (using labelled data), unsupervised learning (finding patterns in unlabelled data), and reinforcement learning (learning from interactions with an environment).[27] At the same time, Deep Learning is a specialised form of machine learning that involves neural networks with multiple layers (deep neural networks). These networks are capable of learning hierarchical representations of data, and they excel at tasks such as image and speech recognition. Deep Learning architectures, like

[22] One Hundred Year Study on Artificial Intelligence (AI100), 2016 Report, STANFORD UNIVERSITY (2016), https://ai100.stanford.edu/2016-report.

[23] Defined.ai, WORLD ECONOMIC FORUM, https://www.weforum.org/organizations/Defined.ai.

[24] National Institute of Standards and Technology, Artificial Intelligence, https://www.nist.gov/artificial-intelligence

[25] Artificial Intelligence Act, 2024, Article 3 (1), Act of Parliament, European Union

[26] Arthur Samuel, Some Studies in Machine Learning Using the Game of Checkers, 3 IBM J. Res. & Dev. 210, 210-229 (1959)

[27] Ibid.

artificial neural networks, consist of interconnected nodes organised into layers.[28] Deep neural networks consist of an initial layer for input, multiple concealed layers, and a final output layer. The inherent depth in these networks facilitates the automatic extraction of features and patterns from data. Inspired by neural connections in the human brain, neural networks are computational systems that enable deep learning. Cognitive computing endeavours to replicate the human thought process within a computer model, striving to enhance the interaction between humans and machines by grasping human language and the significance of images.[29] NLP technology serves as a tool enabling computers to comprehend, recognize, interpret, and generate human language and speech. Regarding Computer Vision, this component leverages deep learning and pattern recognition to interpret the content of images.[30]

Thus, AI is the overarching concept of creating intelligent machines, Machine Learning is a subset of AI focused on algorithms that learn from data, and Deep Learning is a further subset of ML involving neural networks, NLP and computer vision with multiple layers for sophisticated pattern recognition and feature extraction.

INFLUENCE OF AI ON INTERNATIONAL TRADE

AI has undeniably left an indelible mark on various facets of our world, enhancing human capabilities in profound ways. Its influence extends across diverse domains, from finance and national security to healthcare, criminal justice, transportation, and the development of smart cities. Today, various manifestations of AI seamlessly integrate into our daily lives through economic devices and processes. Examples abound, from the voice recognition features on smartphones and smart speakers to content moderation, facial recognition, and biometric identification systems. AI powers online customer service chatbots refines search functions in online shopping and streaming services, facilitate credit scoring, and enables language translation services. Furthermore, it plays a crucial role in the diagnosis and monitoring of healthcare patients and efficiently manages warehouses, shipping, and logistics. The breadth of AI's impact is a testament to its transformative influence on the contemporary human experience.

[28] Yann LeCun, Yoshua Bengio & Geoffrey Hinton, *Deep Learning*, 521 Nature 436, 436-44 (2015)

[29] Ibid.

[30] Tomáš Mikolov et al., *Recurrent Neural Network Based Language Model*, in Interspeech 2010: 11th Annual Conference of the International Speech Communication Association, September 26, 2010

Generally, technology itself has historically played an important role in shaping international trade, but the current explosion in AI has the potential to alter entire global commerce and existing international trade practices. Hence, it can be termed as a disruptive technology in the realm of international trade. AI has the potential to disrupt and transform various facets of international trade, from optimising supply chains and logistics to impacting job markets and trade policies.[31]

➢ APPLICATION OF AI ON GLOBAL SUPPLY CHAINS

AI technologies are already having an impact on the development of supply chain management and logistics operations in the realm of International Trade. Artificial intelligence can enhance inventory management, predict demand, and optimise route planning through specific algorithms and predictive analytic codes. As an illustration, companies can leverage AI to scrutinise prior data, and forecast potential customer demand patterns, enabling them to make necessary adjustments to production levels and streamline their inventory management. Furthermore, AI aids in improving the real-time tracking and monitoring of shipments, thereby affording better oversight and control over the movement of goods. By fine-tuning inventory management and ensuring the right stock levels at the right times, businesses can curtail carrying expenses, avoid stock shortages, and mitigate the risk of excessive stockpiling. AI-driven inventory management systems can autonomously trigger reorders, guaranteeing optimal stock levels while minimising the need for manual intervention. Artificial intelligence can also ascertain the most efficient delivery routes, resulting in reduced travel times and fuel consumption. This level of optimisation leads to improved delivery schedules, reduced transportation costs, and an overall enhancement in supply chain efficiency. AI technologies enable the real-time tracking and monitoring of shipments, delivering heightened visibility and control to enterprises in terms of their supply chains. By utilising AI-enabled devices, sensors, and AI-based analytics, companies can monitor their goods' location, condition, and status throughout the entire transportation process. Furthermore, AI-driven chatbots and virtual assistants empower businesses to provide tailored support and address customer inquiries promptly. These AI tools can offer language assistance, deliver shipping updates, and help customers with any queries or concerns they may have. Additionally, AI algorithms can scrutinize customer data to detect

[31] Emily Jones, *Digital Disruption: Artificial Intelligence and International Trade Policy, Oxford Review of Economic Policy*, 2023, 39,70-84

preferences, purchasing trends, and patterns, allowing businesses to provide customized recommendations and individualized experiences.[32]

Artificial intelligence profoundly impacts the management of supply chains and logistical activities. Through improving inventory control, enhancing route optimization, facilitating real-time monitoring, and the elevation of customer service, AI-based solutions play a crucial role in boosting effectiveness, lowering expenses, and elevating customer contentment. As companies increasingly adopt these technological advancements, the potential for extensive innovation and transformation in the realm of global commerce is considerable.

➢ APPLICATION OF AI ON AUTOMATION OF JOBS

AI-driven technologies possess the capacity to streamline and mechanise repetitive and standardised tasks within various sectors. Although this mechanisation offers certain benefits, it sparks concerns regarding job displacement especially that involves repetitive tasks. Occupations entailing manual labour or routine cognitive duties are especially vulnerable to replacement by AI systems. AI-operated robots and machinery can execute repetitive assembly line procedures in manufacturing, leading to increased productivity and efficiency. This mechanisation can also cut down on business operational expenditures by diminishing errors, enhancing precision, and optimising resource allocation. Tasks that entail manual labour or routine cognitive responsibilities are particularly at risk of being automated. This transformation in the labour market necessitates thoughtful contemplation and proactive actions to mitigate the potential impact on employment.

The mechanisation introduced by AI technologies holds the potential to disrupt the employment landscape, especially in positions that involve repetitive responsibilities. Nonetheless, through proactive steps such as the implementation of retraining and skills enhancement initiatives, individuals can adapt to the evolving demands of the AI-driven economy. By fostering cooperation between humans and AI systems and leveraging the unique strengths of both, societies can navigate labour market disturbances and harness the complete potential of AI in global commerce.[33]

[32] Arindam Bhattacharya, *How AI could Disrupt International Trade, Advocacy Unified Network*, aunetwork.org, (2023)
[33] Ibid.

➢ APPLICATION OF AI ON TRADITIONAL AND DIGITAL MARKETS

AI empowers businesses, both online and conventional, to enhance their ability to analyse market trends, customer expectations, and competitive landscapes with remarkable efficiency. AI technologies utilise big data to analyse the said trends and generate accurate results. The utilisation of data-driven methods plays a pivotal role in shaping strategic decision-making for businesses. It aids in the identification of untapped market potential and potential trade collaborators. Moreover, AI eases international transactions by providing accurate translation services, automating contract management, and enhancing personalised customer behaviours. AI algorithms, through the analysis of big data, have the capability to identify emerging market trends, consumer preferences, and competitive landscapes. These insights enable businesses to customise their products and services to align with market demands, discover new market opportunities, and formulate effective marketing strategies. As we frequently observe in our daily lives, personalised advertisements are delivered through social media. AI can run through social media data to grasp consumer sentiments and preferences, facilitating businesses in tailoring their offerings to specific target audiences. AI algorithms can also assess demographic data, economic indicators, and consumer behaviour patterns to pinpoint market gaps and potential customer segments. This information guides businesses to expand into new territories, establish trade partnerships with previously unexplored markets, and diversify their customer base. The utilisation of automated translation services overcomes language barriers, thereby fostering communication and negotiation with international partners. AI-driven contract management systems can automate contract creation, review, and administration, reducing paperwork and enhancing the efficiency of international trade agreements. Additionally, AI contributes to improved risk assessment and compliance in international trade. AI-powered risk assessment systems can alert businesses to potential trade risks, such as sanctions or regulatory changes, empowering them to make well-informed decisions and take necessary precautions to ensure compliance.

While AI disrupts certain aspects of international trade, it also generates new market dynamics and opportunities. By harnessing AI-powered technologies, companies can access valuable insights into market trends, unearth unexplored markets, streamline cross-border transactions, and enhance risk assessment and compliance procedures. Embracing AI in international trade empowers businesses to make informed decisions, expand into new markets, and deliver personalised customer experiences, ultimately driving growth and success in an increasingly interconnected global economy.

➢ AI AND INTELLECTUAL PROPERTY RIGHTS

The ascent of AI gives rise to challenges in trade policies and intellectual property rights in international trade. As AI innovations and technologies advance, regulating and safeguarding IP rights is more significant. Artificial Intelligence is undeniably reshaping the Intellectual Property landscape, affecting its generation, utilisation, and safeguarding. AI plays a pivotal role in generating fresh intellectual property by facilitating automated content generation across diverse domains such as commerce, the arts, corporate ventures, music, literature, and even scientific investigations. AI algorithms possess the capability to scrutinise extensive datasets, discern recurring patterns, and devise original concepts, blueprints, or innovations, thereby producing innovative intellectual property assets. These AI-driven algorithms have the capacity to scrutinise a wide array of information, including patents, scientific publications, and existing knowledge, in order to pinpoint potential breaches, assess patent viability, conduct intellectual property due diligence, and enhance technology licensing and exchange. AI also offers assistance in the vigilance and identification of intellectual property infringements, as well as the recognition of violations related to copyrights and trademarks. Likewise, AI is a tool for protecting IP, and at the same time, it is itself a subject of IP protection. Artificial intelligence represents a significant intellectual property asset, and safeguarding it requires a combination of tactics, such as patenting innovations in AI, protecting trade secrets, and adhering to copyright regulations for AI-generated content. Establishing a strong foundation for AI-related IP rights is essential to promote innovation and facilitate the utilisation of AI technologies in global commerce.

LEGAL AND ETHICAL CHALLENGES OF AI

Frequently entangled in controversy, the ethical deployment of technology sparks global discussions on various fronts. These dialogues delve into the intricate considerations surrounding the integration of artificial intelligence (AI) into societal frameworks, raising pivotal questions about the appropriate roles for AI in lieu of human involvement. The discourse extends to the safeguarding of personal data and the prevention of potential violations of human rights, prompting inquiries into the responsible collection, utilisation, and purpose of such data.

According to Statista, the revenue from the AI software market worldwide is anticipated to reach a staggering 126 billion dollars by 2025. Concurrently, Gartner reports that 37% of organisations have already implemented AI in some form, with the percentage of enterprises embracing AI experiencing a remarkable 270% growth over the past four years. This accelerating trend reflects the increasing integration of AI across diverse sectors. One noteworthy instance exemplifying the contentious nature of AI implementation occurred in 2023 when the utilisation of AI tools, including ChatGPT, played a central role in triggering a writer's strike. The repercussions were felt significantly across the entertainment industry, leading to disruptions that underscored the broader debate on the ethical implications of AI-generated content.

As businesses grapple with incorporating AI tools into their operations, they confront the intricate challenges of maintaining ethical standards and addressing potential legal ramifications. The absence of well-defined and unequivocal guidelines for the utilisation of AI introduces the risk of misuse and legal entanglements, emphasising the need for a comprehensive framework to govern the responsible deployment of AI technologies.

Additionally, according to Servion Global Solutions, it is projected that by 2025, an astonishing 95% of customer interactions will be powered by AI. This further underscores the pervasive influence of AI across various sectors, emphasising the urgency for ethical considerations and regulatory frameworks to guide the responsible use of AI technologies. A 2022 report from Statista further supports this trajectory, revealing that the global AI software market is expected to grow approximately 54% year-on-year, reaching a forecast size of USD $22.6 billion. These statistics highlight the dynamic nature of the AI landscape, necessitating ongoing dialogues on ethical standards and regulatory frameworks to navigate its evolving role in society.

Some of the major legal and ethical issues relating to AI are:

1. LACK OF ALGORITHMIC TRANSPARENCY

The issue of algorithmic transparency stands as a prominent concern within legal deliberations surrounding artificial intelligence. The increasing integration of AI in high-risk domains intensifies the need to establish accountability, fairness, and transparency in its design and governance. This mounting pressure reflects a growing awareness of the potential repercussions associated with opaque algorithms.[34] The problematic nature of the lack of algorithmic transparency can be seen through instances where individuals faced adverse consequences such as job denials, loan refusals, inclusion on no-fly lists, or denial of benefits, all without understanding the rationale behind these decisions other than their reliance on software-driven processes. This opacity not only leads to unjust outcomes but also leaves affected individuals in the dark about the underlying decision-making mechanisms.[35]

Adding to the complexity of the issue, the information regarding the functionality of algorithms is intentionally obscured, exacerbating the challenges associated with algorithmic transparency. This intentional obscurity hinders public comprehension of AI processes, further fuelling concerns about the fairness and accountability of automated decision-making systems.[36] Consequently, as AI continues to permeate various facets of society, the imperative to address and rectify the lack of algorithmic transparency becomes even more crucial for fostering responsible and ethical AI practices.

2. CYBER SECURITY VULNERABILITIES

The primary cybersecurity concern is the potential for fully automated decision-making, resulting in costly errors and even fatalities. Additionally, there are alarms about the utilisation of AI weapons without human intervention and the risks associated with such autonomous systems. The application of AI to areas like surveillance or national security introduces a novel attack vector termed 'data diet vulnerability.' This vulnerability arises from the increased dependence on AI-driven technologies, creating opportunities for malicious actors to exploit and manipulate sensitive data. [37] Also, there are concerns about the growing deployment of artificial agents for civilian surveillance by governments, exemplified by predictive policing algorithms. These practices have been criticized for their potential infringement on fundamental citizens' rights. The ramifications of these issues extend beyond privacy concerns to encompass the compromise of critical infrastructures, posing severe threats to society and individuals. The potential impacts on life, human

[34] C Cath, *Governing artificial intelligence: Ethical, legal and technical opportunities and challenges, Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, The Royal Society Publishing* (2018)

[35] DR Desai, JA Kroll, *Trust but verify: A guide to algorithms and the law*, Harv. JL & Tech, 31 (2017), p. 1

[36] BD Mittelstadt, P Allo, M Taddeo, S Wachter, L Floridi, *The ethics of algorithms: Mapping the debate*, Big Data & Society (2016)

[37] OA Osoba, W Welser IV, *The risks of artificial intelligence to security and the future of work*, RAND Corporation Santa Monica (2017)

security, and access to essential resources underscore the gravity of these cybersecurity vulnerabilities.[38]

3. UNFAIRNESS, BIAS AND DISCRIMINATION

Issues of unjustness, partiality, and inequity consistently arise and pose a significant hurdle in connection with the utilisation of algorithms and automated decision-making systems. For instance, they are employed in decision-making processes concerning health, employment, credit, criminal justice, and insurance. In August 2020, protests emerged, and legal disputes arose over the use of a controversial exams algorithm, which was implemented to assign grades to GCSE students in England.[39]

A focal document from the EU Agency for Fundamental Rights (FRA 2018) delineates the potential for biased outcomes against individuals through algorithms. It asserts that "the principle of non-discrimination, as articulated in Article 21 of the Charter of Fundamental Rights of the European Union, must be considered when applying algorithms to daily life". A report from the European Parliament on the fundamental rights implications of big data: privacy, data protection, non-discrimination, security, and law enforcement emphasises that due to the data sets and algorithmic systems involved in assessments and predictions at various stages of data processing, big data may lead to violations of individual rights and differential treatment, indirectly discriminating against groups with similar characteristics. This is particularly relevant to fairness and equal opportunities in education and employment, recruitment or assessment of individuals, and the determination of new consumer habits among social media users. The report urges the European Commission, Member States, and data protection authorities to identify and implement measures to minimise algorithmic discrimination and bias. It also calls for the development of a robust and shared ethical framework for the transparent processing of personal data and automated decision-making, guiding data usage and ensuring the continual enforcement of Union law.[40]

[38] H Couchman, *Policing by machine, Predictive Policing and the threats to our rights* (2019)
[39] The Guardian, *Controversial exams algorithm to set 97% of GCSE results*, The Guardian (Aug. 15, 2020), https://www.theguardian.com/education/2020/aug/15/controversial-exams-algorithm-to-set-97-of-gcse-results
[40] European Parliament, *Resolution of 14 March 2017 on Fundamental Rights Implications of Big Data: Privacy, Data Protection, Non-Discrimination, Security and Law-Enforcement*, 2016/2225(INI) (2017)

4. LACK OF CONTESTABILITY

Contestability here refers to the ability to challenge and question the outcomes or decisions made by AI systems. The absence of contestability will hinder individuals' rights to appeal or seek redress when adversely affected by automated decisions. The absence of an evident means to challenge automated systems when they generate unexpected, harmful, unfair, or discriminatory outcomes can be called the lack of contestability.[41] The lack of transparency in machine learning systems could diminish both the accountability of their 'owners' and the contestability of their decisions.[42] In an article by E Bayamlıoğlu, he argues that "a satisfactory standard of contestability will be essential in the face of a threat to individual dignity and fundamental rights" and that the 'human element' of judgment is, for certain decision types, an indispensable aspect of legitimacy.[43] Reviewability and contestability are considered concurrent with the rule of law and, therefore, vital prerequisites for democratic governance.

5. LEGAL PERSONHOOD ISSUES

As AI systems become increasingly sophisticated and autonomous, there is a growing debate about whether they should be granted some form of legal personhood. Proponents in favour of granting argue that this recognition is essential for defining clear lines of responsibility when AI systems make decisions or engage in actions that impact individuals or society. Granting legal personhood could facilitate holding AI entities accountable for their actions, allowing for legal recourse in cases of harm or wrongdoing. According to them, bestowing legal personality upon AI could serve as a nuanced solution to practical challenges in assigning responsibility for AI actions or supporting the potential moral rights of AI entities.[44] L Jaynes, an eminent in the AI field, envisions a future where artificial entities attain even citizenship. In the European Union, there is a prevalent cautionary sentiment against creating a new legal personality for AI systems.[45]

[41] L Edwards, M Veale, *Slave to the algorithm? Why a "right to an explanation" is probably not the remedy you are looking for*, Duke Law and Tech Review, 16 (2017), pp. 18-84

[42] M Hildebrandt, *The new imbroglio: Living with machine algorithms*, The Art of Ethics in the Information Society, 55-60 (2016),

[43] E Bayamlıoğlu, *Contesting automated decisions*, European Data Protection Law Review, 4, 433-446 (2018)

[44] J Turner, *Robot Rules: Regulating Artificial Intelligence*, Legal personality for AI, 173-205 (2019),

[45] K Siemaszko, R Rodrigues, S Slokenberga, *D5.6: Recommendations for the enhancement of the existing legal frameworks for genomics, human, enhancement, and AI and robotics*, SIENNA project (2020)

Critics against the granting, argue that extending personhood to AI could blur the lines between machines and humans, potentially undermining the core principles that underpin legal systems. Questions about AI's capacity for ethical reasoning, emotional understanding, and moral agency further complicate the issue. The High-Level Expert Group on Artificial Intelligence (AI HLEG) of the EU strongly advises against granting legal personality to AI systems or robots. According to them, doing so would contradict the principles of human agency, accountability, and responsibility, posing a substantial moral hazard.[46] Striking the right balance between acknowledging the autonomy of AI and preserving human-centric legal frameworks remains a significant challenge for lawmakers and ethicists alike.

6. INTELLECTUAL PROPERTY ISSUES

AI plays a pivotal role in generating fresh intellectual property by facilitating automated content generation across diverse domains such as commerce, the arts, corporate ventures, music, literature, and even scientific investigations. AI algorithms possess the capability to scrutinise extensive datasets, discern recurring patterns, and devise original concepts, blueprints, or innovations, thereby producing innovative intellectual property assets. These AI-driven algorithms have the capacity to scrutinise a wide array of information, including patents, scientific publications, and existing knowledge, in order to pinpoint potential breaches, assess patent viability, conduct intellectual property due diligence, and enhance technology licensing and exchange. AI also offers assistance in the vigilance and identification of intellectual property infringements, as well as the recognition of violations related to copyrights and trademarks. Questions arise about whether AI's inventions should be recognised as prior art, the ownership of datasets crucial for an artificial intelligence's learning process, and identifying responsibility for creativity and innovation arising from AI, particularly when they infringe upon the rights of others or contravene legal provisions. Likewise, AI is a tool for protecting IP, and at the same time, it is itself a subject of IP protection. Artificial intelligence represents a significant IP asset, and safeguarding it requires a combination of tactics, such as patenting innovations in AI, protecting trade secrets, and adhering to copyright regulations for AI-generated content. Establishing a strong foundation for AI-related IP rights is essential to promote innovation and facilitate the

[46] European Commission, *Policy and Investment Recommendations for Trustworthy Artificial Intelligence*, Digital Single Market, https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence (last visited June 16, 2024)

utilisation of AI technologies in global commerce. A lawsuit was filed against Alphabet Inc., Google Deepmind, and Google LLC on July 11, 2023, in Northern District of California, alleging that Google unlawfully utilized content from millions of Americans to develop AI technologies like Bard, giving Google an unfair competitive edge over rivals who acquire data through legal means for AI training. The lawsuit suggests potential damages exceeding $5 billion.[47] In a similar lawsuit against OpenAI, Inc. and others, alleges that OpenAI utilized copyrighted books to train its large language models, including ChatGPT. The court finds it very hard to decide on the case.[48]

The advent of machine learning, deep learning, and AI has propelled innovation to new heights. However, a complex issue arises when the inventor is, in fact, an artificial entity. The patent system essentially bestows a monopoly upon the AI inventor, granting them the capacity to exploit the invention for commercial purposes. Intellectual property laws establish this recognition as a reward for the innovation introduced by the inventor. Getty Images (US), Inc. filed a lawsuit on February 3, 2023, in U.S. District Court of Delaware against Stability AI, Inc., alleging infringement of copyrighted photographs and trademarks. Getty claims Stability AI used over 12 million images from Getty's website to train Stable Diffusion despite explicit usage terms prohibiting such actions.[49] Also in Andersen et al. v Stability AI Ltd., Midjourney, Inc., and DeviantArt, Inc.,[50] the court checked the unauthorized use of plaintiff's works to train various AI image generators. Plaintiffs argue that AI outputs constituted unauthorized derivative works and claim vicarious copyright infringement, asserting violations of the DMCA by altering or removing copyright management information.

Currently, many well-developed countries leverage AI software to enhance their innovative capabilities, even permitting AI to play an integral role in generating inventions. If these AI-driven inventions remain unpatentable due to the involvement of AI, the substantial investments of both time and financial resources dedicated to their development come into question. The prevailing reality is that AI primarily serves as a facilitator for extensive database management and simulation during the invention process. This amalgamation of human creativity and machine learning capabilities are combined to foster innovation. But there is an actual instance where the inventor of an innovation is an AI machine. In the landmark case of DABUS (an AI system that stands for Device for the Autonomous Bootstrapping of Unified Sentience), created by Dr. Stephen Thaler, the applicant was the AI machine itself. The patent offices of the USA, England, and Australia

[47] J.L. v. Alphabet Inc., No. 3.23-cv-03440 (N.D. Cal. July 11, 2023)
[48] Silverman et al. v. OpenAI Inc. et al., No. 3:23-cv-03416 (N.D. Cal. July 7, 2023)
[49] Getty Images (US), Inc. v. Stability AI, Inc., 1:23-cv-00135, (D. Del.)
[50] *Andersen v. Stability AI Ltd.*, 23-cv-00201-WHO (N.D. Cal. Oct. 30, 2023)

have rejected the application on the basis that the inventor should be a natural person and not a machine. At last, this AI machine was granted a patent from South Africa on July 28, 2021.[51] However, there are still some fusses regarding the decision around the world of IP and technological experts. Even the Australian courts have recently held that AI is capable of being an 'inventor'.[52]

Likewise, the question of whether artistic creations produced by artificial intelligence can be afforded copyright protection remains a subject of debate. Notably, the United States Copyright Office has recently promulgated regulations governing the incorporation of AI in newly generated artistic works, stipulating that copyright is only applicable to the portions directly authored by humans, excluding AI-generated content. In the seminal case of Infopaq International A/S vs. Danske Dagblades Forening (2009)[53], the Court of Justice of the European Union held that protection for works originating from computer programs is contingent upon the inclusion of the author's creativity. Similarly, in Kadery et al. v Meta Platforms, Inc.,[54] it was held that Facebook was using copyrighted books to train its LLaMA program, launched in February 2023.

While AI-generated creations aren't explicitly barred from copyright protection under existing laws, these regulations primarily favour creative outputs with a human touch. At present, when AI generates content that showcases artistic originality, the copyright is typically attributed to the human element behind the work, as AI essentially emulates what it has been trained on without contributing genuine novelty. This is because the creative content produced by AI often closely resembles the data it has learned from. A suit against GitHub, Inc., Microsoft, and OpenAI, alleged violations of DMCA Section 1202 through unauthorized use of programmers' software code to develop AI systems like Codex and Copilot.[55] Nonetheless, if AI is not considered the rightful author, ownership of such creations may likely fall to either the individual who programmed the AI system or the one who supplied the data that served as the basis for the AI-generated work. Anyway, the

[51] Lynsey Chutel, *South Africa Grants Patent to an AI System Known as DABUS*, Quartz (July 30, 2021), https://qz.com/africa/2044477/south-africa-grants-patent-to-an-ai-system-known-as-dabus/

[52] Rebecca Currey & Jane Owen, *Australian Court Finds AI Systems Can Be "Inventors"*, WIPO Magazine (Sept. 2021), https://www.wipo.int/wipo_magazine/en/2021/03/article_0006.html.

[53] Case C-5/08, Infopaq Int'l A/S v. Danske Dagblades Forening, 2009 E.C.R. I-6569

[54] Kadrey et al. v. Meta Platforms, Inc., No. 3:23-cv-03417 (N.D. Cal. July 7, 2023)

[55] *Doe v. GitHub, Inc.*, 22-cv-06823-JST (N.D. Cal. Jan. 3, 2024)

implication of AI on Copyright is far-reaching and will be drastically changing in the near future.

7. ADVERSE EFFECTS ON WORKERS AND LABOURERS

The 2017 report from the IBA Global Employment Institute underscores the global apprehension regarding the influence of AI and robotics on the workforce.[56] Various concerns have been identified, encompassing alterations in the prerequisites for prospective employees, a decline in the demand for workers, shifts in labour relations, emergence of novel job structures and categories, employee layoffs, disparities in the 'new' job market, assimilation of unskilled workers into the 'new' job market, potential ramifications for union activities and collective bargaining, challenges for employee representatives, transformations in union structures, health and safety considerations, effects on working hours, modifications in remuneration and pensions, and social security challenges. There is the possibility of workers experiencing a significant loss of autonomy.[57]

These challenges extend beyond mere economic implications such as poverty, extending into profound social consequences like homelessness, displacement, violence, and despair. Additionally, there is a considerable potential for human rights impacts, posing ethical quandaries that, although challenging, must be addressed due to their critical nature.

8. PRIVACY AND DATA PROTECTION ISSUES

Legal scholars and regulatory bodies focused on data protection assert that AI, while impacting various rights, presents substantial challenges in the realms of privacy and data protection.[58] AI systems increasingly rely on vast amounts of data to enhance their learning and decision-making processes, and the collection and utilisation of personal information become more prevalent. This creates a complex web of ethical and legal challenges, as individuals grapple with the potential invasion of their privacy. These challenges encompass issues such as obtaining informed consent, concerns related to surveillance, and potential violations of individuals' data protection rights.[59] These encompass the right to access

[56] International Bar Association Global Employment Institute, *Artificial Intelligence and Robotics and Their Impact on the Workplace* (2017). https://www.ibanet.org/Document/Default.aspx?DocumentUid=c06aa1a3-d355-4866-beda-9a3a8779ba6e

[57] Royal Society, Frontier Review: The Impact of AI on Work, https://royalsociety.org/-/media/policy/projects/ai-and-work/frontier-review-the-impact-of-AI-on-work.pdf (last visited June 16, 2024)

[58] S Gardner, *AI poses big privacy and data protection challenges*, Bloomberg Law News, (2016)

[59] Brundage M, *The malicious use of artificial intelligence: forecasting, prevention, and mitigation*, (2018)

personal data, the right to prevent processing that may result in harm or distress, and the right to avoid decisions made solely through automated processes, among various others.

Machine learning algorithms, a subset of AI, often require extensive datasets for training, which may include sensitive information such as personal preferences, behaviours, and even biometric data. The indiscriminate use of such data poses a risk of unauthorised access, misuse, or even malicious intent. Additionally, the opacity of some AI algorithms exacerbates the privacy dilemma. Deep learning models, for instance, are often considered "black boxes" due to their complexity, making it challenging to discern how they arrive at specific conclusions. This lack of transparency raises concerns about the potential for biased decision-making or the inadvertent perpetuation of existing societal prejudices, further compromising individual privacy. Furthermore, the aggregation of data from various sources for AI applications poses a risk of creating comprehensive profiles of individuals, leading to a loss of anonymity and an increased potential for exploitation.

In the context of the 38th International Conference of Data Protection and Privacy Commissioners in 2016, the European Data Protection Supervisor (EDPS) background document on Artificial Intelligence, Robotics, Privacy, and Data Protection underscores the potential escalation of privacy implications and the enhanced capabilities of surveillance. Furthermore, the Information Commissioner's Office (ICO) of the United Kingdom, in its discussion paper on Big Data, Artificial Intelligence, Machine Learning, and Data Protection, explores the ramifications of these technologies.[60] According to the report, the analysis of big data using techniques made possible by AI creates implications for data protection, and it can be more challenging to apply the data protection principles when using personal data in a big data context.[61] These consequences emerge not just due to the sheer amount of data but also because of how it is produced, the inclination to discover novel applications for it, the intricacy of the processing involved, and the potential for unforeseen outcomes affecting individuals.[62]

[60] European Data Protection Supervisor, *Artificial Intelligence, Robotics, Privacy, and Data Protection,* Room document for the 38th International Conference of Data Protection and Privacy Commissioners (October 16, 2019), https://www.edps.europa.eu/sites/default/files/publication/16-10-19_marrakesh_ai_paper_en.pdf.

[61] Ibid

[62] .

9. LIABILITY FOR DAMAGE

The implementation and utilisation of AI technologies have the potential to inflict harm upon individuals and assets. There are instances of this perilous impact, including accidents such as pedestrians being struck by autonomous vehicles, collisions and damages resulting from the partial operation of drones, and the erroneous diagnosis of medical conditions due to AI software programs.[63] A multitude of stakeholders are identified within an AI system, including the data provider, designer, manufacturer, programmer, developer, user, and the AI system itself. The intricate interplay among these entities complicates the attribution of liability when unforeseen events occur. The complexity of the AI ecosystem underscores the challenge of establishing accountability when mishaps transpire, requiring careful consideration of numerous contributing factors.

10. LACK OF ACCOUNTABILITY FOR HARMS

For ensuring accountability in the realm of AI there is a need for the establishment of mechanisms to oversee the development, deployment, and utilisation of AI systems. This involves the implementation of robust risk management strategies aimed at identifying and mitigating potential risks in a transparent manner, enabling third-party scrutiny and auditability.[64] Adding further depth to this perspective, Dignum emphasises that accountability in AI encompasses not only the guidance of actions through belief formation and decision-making but also the explanation of decisions within a broader context and their classification based on moral values.[65] Highlighting the practical difficulties in ensuring accountability, a report by Privacy International and Article 19 (2018) underscores the challenges faced even when potential harms are identified. The report suggests that holding those responsible accountable for violations becomes intricate, further emphasising the complexities involved in addressing accountability concerns within the AI landscape.

[63] Gluyas L, Day S, *Artificial Intelligence - Who Is Liable When AI Fails To Perform?* CMS Cameron McKenna Nabarro Olswang LLP (2018). https://cms.law/en/GBR/Publication/Artificial-Intelligence-Who-is-liable-when-AI-fails-to-perform

[64] European Commission, *Assessment List for Trustworthy Artificial Intelligence (ALTAI): Self-Assessment*, https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment (last visited December 6, 2023)

[65] V Dignum, *The art of AI—accountability, responsibility and transparency,* Medium (2018), https://medium.com/@virginiadignum/the-art-of-ai-accountability-responsibility-transparency-48666ec92ea5

CONCLUSION

In this chapter, we looked at the history and landscape surrounding AI, the different ways people define Artificial Intelligence, and how this disruptive technology affects international trade. Significantly, the legal and ethical challenges arising from the integration of AI were analysed, unravelling the intricate dilemmas faced by policymakers, legal practitioners, ethical theorists and people in general. As we navigate through these complexities, it becomes evident that the intersection of AI and international trade demands a thoughtful and adaptive legal framework, one that can aptly address emerging challenges while fostering innovation and equitable global trade relations. The ensuing chapters will further refine our understanding and propose informed recommendations to navigate this intricate terrain at the intersection of law, ethics, and technological progress.

CHAPTER 3

AI REGULATORY INITIATIVES AROUND THE WORLD

INTRODUCTION

Artificial intelligence, which is developing at a disruptive pace, has been integrated into several industries and sectors, offering revolutionary possibilities. The previous chapter analysed the remarkable benefits and opportunities that AI specifically provides for international trade. However, the rapid growth of this expansion also gives rise to ethical concerns, including issues such as potential biases, privacy infringements, and safety hazards. Governments worldwide are increasingly recognising the significance of legislative frameworks in addressing these concerns and ensuring the ethical and responsible development and implementation of AI technologies. To comprehend the worldwide impact of AI, developers and implementers worldwide must acquaint themselves with the existing legal initiatives and governance frameworks that regulate AI. Furthermore, this comprehension spans the realm of worldwide legislation and international rules regarding artificial intelligence, which acts as a crucial foundation for navigating the ever-changing landscape of AI governance. The implementation of international rules promotes cooperation, mitigates tensions, and upholds moral standards in the utilisation of AI. Common criteria for privacy, accountability, openness, and data protection are necessary to establish a unified framework for AI compliance. Global regulations on artificial intelligence have the potential to greatly improve international cooperation, promote innovation, and mitigate the risks posed by a fragmented regulatory system. The fundamental focus of this discussion is the concept of "Global AI Oversight," which emphasises the need for international frameworks and rules to monitor the development and implementation of AI on a worldwide level.[66] There has been a growing acknowledgement in recent years of the necessity for ethical and responsible behaviours in the field of AI on a global scale.[67] Several institutions are actively promoting international regulation on AI in this context. The United

[66] IT Exchange, *AI Regulatory Initiatives Around the World: An Overview*, IT Exchange (2023), https://www.itexchangeweb.com/blog/ai-regulatory-initiatives-around-the-world-an-overview

[67] MENA Report, Slovenia: The Prime Minister: "*Everyone - governments, the science, the business sector and academics - has the opportunity in our hands to develop and direct artificial intelligence for the benefit of humanity.*" (2020).

Nations (UN) has initiated deliberations on the ethical and regulatory aspects of AI through its specialist agencies such as UNICRI[68] and UNESCO[69]. In comparison, the European Union (EU) has emerged as a leading proponent of creating new regulations for AI that prioritise ethical AI development and a focus on human well-being. This chapter will examine the contemporary international legal frameworks that regulate AI and analyse the specific legal regulations in various significant worldwide regions.

INTERNATIONAL REGULATIONS

➢ UNITED NATIONS

The United Nations General Assembly on 21st March 2024 unanimously adopted the first global resolution on AI to encourage the protection of personal data, the monitoring of AI for risks, and the safeguarding of human rights.[70] Introduced by the United States and backed by 123 nations, the resolution gained consensus bypassing the need for a formal vote. This indicates the unanimous support of all 193 UN member states. This resolution is part of a series of governmental efforts worldwide to influence the trajectory of AI development, addressing concerns regarding its potential to disrupt democratic processes, facilitate fraud, or precipitate significant job displacement, among other potential negative impacts. This initial worldwide resolution on artificial intelligence, unanimously approved by the UN General Assembly, aims to promote the protection of personal information, the vigilant monitoring of AI risks, and the preservation of human rights. The resolution further seeks to bridge the gap in access to digital resources between affluent developed nations and less prosperous developing nations, ensuring their equitable participation in AI discussions. Additionally, it strives to equip developing nations with the necessary technology and skills to harness the advantages of AI, such as disease detection, flood prediction, agricultural assistance, and workforce training for future generations.[71] Even though it is not binding,

[68] United Nations Interregional Crime and Justice Research Institute (UNICRI), *AI Against Crime: Leveraging Artificial Intelligence and Machine Learning to Fight Crime*, (2020). https://unicri.it/sites/default/files/2020-08/Artificial%20Intelligence%20Collection.pdf

[69]. United Nations Educational, Scientific and Cultural Organization (UNESCO), *Ethics of Artificial Intelligence* (April 22, 2024). https://www.unesco.org/en/artificial-intelligence/recommendation-ethics#:~:text=The%20use%20of%20AI%20systems,may%20result%20from%20such%20uses.&text=Unwanted%20harms%20(safety%20risks)%20as,and%20addressed%20by%20AI%20actors.

[70] General Assembly Adopts Landmark Resolution on Steering Artificial Intelligence towards Global Good, Faster Realization of Sustainable Development | Meetings Coverage and Press Releases. (March 21, 2024). https://press.un.org/en/2024/ga12588.doc.htm

[71] United Nations Adopts Its First Resolution on AI, Baker McKenzie Insight Plus (April 24, 2024), https://www.globalcompliancenews.com/2024/04/24/https-insightplus-bakermckenzie-com-bm-data-

the resolution urges various stakeholders, including nations, international bodies, technology communities, civil society, media, educational institutions, and individuals, to devise and endorse regulatory and governance mechanisms for ensuring the safety of AI systems. It cautions against the inappropriate or malicious creation, development, deployment, and utilization of artificial intelligence systems, particularly in cases where adequate precautions are lacking or when actions contradict international laws. Another objective outlined in the resolution is leveraging AI to accelerate progress towards fulfilling the United Nations' 2030 development objectives[72], which encompass eradicating global hunger and poverty, enhancing global health standards, providing quality secondary education to all children, and attaining gender equality. The resolution urges the 193 member states of the United Nations and other entities to support developing nations in accessing the advantages of digital transformation and secure AI technologies. It stresses the importance of upholding human rights and fundamental freedoms throughout the entire lifecycle of AI systems.

The established its specialized Centre for AI and Robotics in September 2017, with backing from various entities, including the Municipality of the Hague, and strategic partners.[73] This initiative aims to deepen comprehension regarding the potential risks and benefits associated with AI, robotics, and related technologies concerning crime, terrorism, and security threats. UNICRI, leveraging its status as a UN entity, has orchestrated numerous events to foster awareness and discourse on these matters. These include high-profile events at the UN Headquarters, workshops on identifying programmatically generated content like deepfakes, and training sessions tailored for the judiciary and journalists. Moreover, UNICRI has facilitated multi-stakeholder dialogues on the convergence of AI and national security, alongside symposiums in collaboration with Interpol concerning AI's role in law enforcement. Furthermore, UNICRI's endeavours extend to conceptualizing and developing AI-based tools geared towards preventing, detecting, and aiding in the prosecution of perpetrators involved in online child sexual exploitation and deciphering anomalies in financial transactions indicative of terrorism financing. Through these multifaceted

technology-international-the-united-nations-adopts-its-first-resolution-on-ai_04152024-2/#:~:text=In%20brief,intelligence%20systems%20for%20sustainable%20development%E2%80%9D

[72] UN Development Programme: Sustainable Development Goals, United Nations Development Programme, https://www.undp.org/sustainable-development-goals

[73] UNICRI, Centre for Artificial Intelligence and Robotics, "In Focus," https://unicri.it/in_focus/on/unicri_centre_artificial_robotics.

initiatives, UNICRI endeavours to steer Member States towards responsibly harnessing the potential of AI and related technologies while mitigating associated risks.

In 2017, the United Nations Human Rights Council (UNHRC) released two pivotal reports shedding light on the intersections of AI and human rights, a topic of growing concern. These reports, along with submissions from the Office of the High Commissioner for Human Rights and the Independent Expert on the Rights of Older Persons, underscored the potential implications of AI on fundamental rights.[74] They particularly emphasized the inherent biases and discriminatory tendencies that could permeate AI algorithms. Moreover, the reports didn't just dwell on the negative aspects; they also explored how AI could positively impact areas like women's health and the care of older individuals. Efforts continued in subsequent years, notably in 2016 and 2018, with significant amendments to the Vienna Convention on Road Traffic, 1968. These amendments facilitated the adoption of technologies allowing vehicles to assume driving tasks autonomously, provided they adhere to UN vehicle regulations and grant drivers the ability to override or deactivate such systems when necessary. This marked a significant step forward in ensuring the safe integration of AI in transportation while upholding human rights principles.

On 15th September, 2023, the United Nations Educational, Social and Cultural Organisation (UNESCO), a specialized agency of the United Nations, issued a call for immediate government intervention and inclusive policy development concerning the integration of AI in the education sector.[75] Highlighting various challenges associated with the growing utilization of generative AI, UNESCO emphasized the necessity of a comprehensive, multi-stakeholder approach to regulate its use effectively. Central to this approach is the prioritization of human-centred principles in crafting regulatory frameworks and policies aimed at fostering equitable AI deployment in education. These policies should facilitate broad access to educational resources, promote personalized and flexible learning opportunities, elevate educational standards, oversee learning processes, and promote ethical AI practices. Building upon the regulatory strategies implemented by different nations since the previous November, UNESCO put forth several recommendations for both regulating and optimizing AI's role in education:

[74] Daniel Cullen, *Why Artificial Intelligence Is Already a Human Rights Issue*, Oxford Human Rights Hub (2018), http://ohrh.law.ox.ac.uk/why-artificial-intelligence-is-already-a-human-rights-issue/

[75] UNESCO, *Governments must quickly regulate Generative AI in schools*. (September 8, 2023) https://www.unesco.org/en/articles/unesco-governments-must-quickly-regulate-generative-ai-schools

1. Establishing a legal framework to safeguard data protection and privacy.
2. Implementing national AI strategies tailored to the education sector.
3. Developing specific regulations addressing the ethical use of AI.
4. Reviewing and strengthening copyright laws to align with AI advancements.
5. Prioritizing capacity-building initiatives and conducting thorough assessments of AI's impact on education.[76]

- INTERNATIONAL TELECOMMUNICATION UNION

The International Telecommunication Union (ITU) is deeply involved in exploring the impact of AI on telecommunications, radiocommunication networks, and the broader landscape of Information and Communication Technology (ICT). ITU conducts regular regulatory surveys to monitor the proliferation of national AI strategies and policies. Given that machine learning models heavily rely on data, national regulations concerning data privacy, protection, and IoT frameworks, alongside the development of 5G networks enabling data transmission, are crucial considerations in shaping national AI approaches. ITU's efforts extend to collecting and disseminating information on effective and sustainable AI solutions, empowering stakeholders with evidence and knowledge for adoption and utilization.[77] Collaborating with organizations like the Food and Agriculture Organization (FAO), ITU publishes reports such as the e-Agriculture in Action Report: AI for Agriculture, spotlighting informative case studies and insights on implementing AI in agriculture.[78] Furthermore, ITU actively deploys and tests promising AI applications to support the provision of services aligned with Sustainable Development Goals (SDGs). For instance, in Senegal, ITU collaborates with WHO and the Ministry of Health and Social Action to pilot test an AI application for the automatic detection of diabetic retinopathy, aiming to enhance screening coverage and accessibility. The release of the AI and big data for development 4.0 report by ITU underscores opportunities and offers policy and regulatory recommendations,

[76] Miao, F., Holmes, W., Huang, R., Zhang, H., & U, *AI and education*, UNESCO Publishing, (April 8, 2021) http://books.google.ie/books?id=yyE7EAAAQBAJ&printsec=frontcover&dq=AI+and+education:+guidance+for+policy-makers&hl=&cd=1&source=gbs_api

[77] International Telecommunication Union, Artificial Intelligence, https://www.itu.int/en/action/ai/Pages/default.aspx

[78] ITU Telecommunication Development Sector, *Digital Agriculture: Harnessing the Power of AI for Agriculture*, (2020) https://www.itu.int/en/ITU-D/ICT-Applications/Documents/Publications/DigitalAgriculture_AI4Agri.pdf

emphasizing the need for governance, ethical considerations, digital skills, and international collaboration in building robust national AI and data systems for development.[79]

- ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The Organisation for Economic Co-operation and Development (OECD) Council's Recommendation on AI, commonly referred to as the "OECD AI Principles," represents a significant international effort to establish a framework for the responsible development and deployment of AI technologies.[80] Adopted in 2019 by the OECD's 36 member countries and endorsed by several non-member countries, the principles aim to guide governments, industry stakeholders, and other relevant actors in harnessing the benefits of AI while addressing its associated challenges. The OECD AI Principles consist of five overarching principles that emphasize Human-centric values, Transparency, Accountability, Robustness, security, and safety and Inclusiveness. These principles serve as a foundation for the responsible stewardship of AI and provide guidance for policymakers, businesses, and other stakeholders in navigating the complex landscape of AI governance. While they are not legally binding, the OECD AI Principles represent a consensus among member and non-member countries on the core values and priorities that should underpin AI development and deployment globally. In addition to the principles themselves, the OECD provides accompanying guidance to support their implementation, including practical recommendations for policymakers and industry stakeholders. By adhering to the OECD AI Principles, countries and organizations can contribute to the responsible and beneficial advancement of AI technologies for the benefit of society as a whole. The Organisation for Economic Co-operation and Development's AI principles have been reaffirmed in many different contexts, including by digital and technology ministers of the G7 countries during the 2023 Hiroshima Summit.[81]

AFRICAN UNION

The African Union High-Level Panel on Emerging Technologies (APET) and the African Union Development Agency (AUDA-NEPAD) organised a Writing Workshop in Kigali, Rwanda, from February 27 to March 3, 2023. The purpose of the workshop was to

[79] ITU-T Recommendation E.800, "Definitions of Terms Related to Quality of Service," Int'l Telecomm. Union (Sept. 2008), http://handle.itu.int/11.1002/pub/81886d62-en

[80] OECD AI Policy Observatory, OECD Principles on Artificial Intelligence, OECD (2023), https://oecd.ai/en/ai-principles

[81] OECD, *G7 Hiroshima Process on Generative Artificial Intelligence (AI): Towards a G7 Common Understanding on Generative AI*, OECD Publishing, Paris, (2023), https://doi.org/10.1787/bf3c0c60-en.

bring together African Artificial Intelligence experts and finalise the drafting of the African Union Artificial Intelligence (AU-AI) Continental Strategy for Africa. The objective is to formulate an all-encompassing plan that would provide guidance to African nations on how to facilitate inclusive and sustainable AI-driven socio-economic change. An AI-powered socio-economic strategy has the capacity to stimulate economic expansion and progress by generating novel industries and employment opportunities, enhancing productivity, and optimising efficiency, hence resulting in heightened prosperity and improved living standards for the entire African population.[82]

In March 2024, the Artificial Intelligence Unit of the Council of Europe contributed to the OECD-African Union Artificial Intelligence Dialogue, hosted in Paris with the support of the United Kingdom. This event showcased the efforts of the Committee on Artificial Intelligence (CAI), drawing together representatives from the AU Commission, AU AI Working Group, and various experts to deliberate on the AU's Continental Strategy for AI in Africa, emphasizing AI governance, collaborative initiatives, and addressing common challenges. African government heads anticipate the endorsement of the continental AI strategy during the AU's annual summit in Ethiopia, which is slated for February 2025. Subsequently, nations lacking existing AI policies will utilize this blueprint to formulate their own strategies, while those with established regulations will be encouraged to realign with the AU's directives. This collective effort underscores the AU's commitment to fostering responsible and beneficial AI development across the continent.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION AND INTERNATIONAL ELECTROTECHNICAL COMMITTEE

The International Organization for Standardization (ISO) and the International Electrotechnical Committee (IEC) released the first of its kind global standard for AI management systems in January 2024.[83] This milestone marks a significant stride towards structuring and supervising AI systems in a prudent, ethical, and transparent manner, all while upholding data privacy and information security. Although lacking legal enforcement, ISO/IEC standards wield substantial influence in the global business sphere, offering

[82] AUDA-NEPAD, Artificial Intelligence is at the Core of Discussions in Rwanda as the AU High-Level Panel on Emerging Technologies Convenes Experts to Draft the AU-AI Continental Strategy, https://www.nepad.org/publication/artificial-intelligence-core-discussions-rwanda-au-high-level-panel-emerging (last visited January 5, 2024) https://www.nepad.org/news/artificial-intelligence-core-of-discussions-rwanda-au-high-level-panel-emerging

[83] P., *ISO/IEC 42001 Explained: Building Trust in AI Systems*, https://pecb.com/article/isoiec-42001-explained-building-trust-in-ai-systems (last visited January 12, 2024)

invaluable guidance to entities involved in developing, providing, or utilizing AI-based products and services. These standards aim to ensure consistent, clear, and responsible management practices throughout the lifecycle of AI systems. Since 2017, the ISO and IEC have joined forces to formulate AI standards.[84] These efforts have laid the groundwork for frameworks such as the AI Risk Management Framework (AI RMF) in the USA,[85] which draws heavily from ISO's risk management standards and the terminology standards established by ISO/IEC. Similarly, these standards also influence the risk management approach outlined in the EU AI Act. The initial edition of the standard, released in December 2023, addresses various facets of artificial intelligence, presenting an integrated strategy for understanding and mitigating risks associated with deploying AI systems within organizational settings. However, standards are not static entities; they evolve over time in response to legislative developments, market trends, and emerging risks. As such, the new AI standard is poised to undergo further refinement, potentially influenced by forthcoming regulations like the AI Regulation. An integral component of the standard pertains to planning, underscoring the importance of deliberate and proactive management practices, including comprehensive risk assessment and impact evaluation. This aligns closely with existing requirements in other domains, such as the data protection impact assessment mandated by Article 35 of the General Data Protection Regulation (GDPR).[86]

Central to the standard is the development and implementation of AI policies by organizations. These policies serve to establish a structured approach to managing AI systems, encompassing ethical considerations, transparency, continuous learning, risk management, and governance. By adhering to these policies, organizations can foster the ethical development and utilization of AI technology, demonstrate accountability, and cultivate transparency and reliability in their AI-related endeavours. Furthermore, the standard underscores the importance of allocating adequate resources and fostering competence and awareness among personnel involved in AI-related activities. Organizations must ensure they possess sufficient resources, including personnel and facilities, to support the effective governance of AI systems. Additionally, personnel engaged in AI-related tasks should possess the requisite competence, education, and awareness regarding ethical

[84] International Telecommunication Union, *AI (Artificial Intelligence) Standardization*, https://www.itu.int/en/ITU-T/AI/Pages/default.aspx

[85] NIST, *AI Risk Management Framework* (January 5, 2024), https://www.nist.gov/itl/ai-risk-management-framework

[86] General Data Protection Regulation (GDPR), Art. 35 – Data protection impact assessment, 2016

considerations, transparency, and the imperative for continuous learning associated with AI technology. In a broader context, these standards serve as benchmarks for quality and sustainability, influencing businesses' decisions when procuring services. They serve as indispensable tools for fostering continual improvement and adherence to best practices over time. The collaborative efforts of ISO and IEC have culminated in the establishment of a global standard for AI management systems, providing essential guidance for organizations seeking to navigate the complexities of AI implementation while upholding ethical principles and regulatory compliance.[87]

US-EU AI CODE OF CONDUCT

The AI Code of Conduct, a collaborative effort between the United States and the European Union, emerges as a pivotal initiative aiming to establish voluntary guidelines for businesses venturing into AI development.[88] This endeavour seeks to bridge regulatory disparities across jurisdictions by formulating non-binding international standards and pre-empting the enactment of formal legislation in respective nations. Margrethe Vestager, the European Union's then Executive Vice President overseeing competition and digital strategy, disclosed this development on May 31, 2023, marking the conclusion of the fourth US-EU Trade & Tech Council meeting. Vestager emphasized the collaborative nature of the initiative, focusing on risk assessment, transparency, and other pivotal facets of AI development. Upon finalization, the AI Code of Conduct intends to be presented to G7 leaders, urging companies to voluntarily adhere to its principles. Further, in the sixth TTC Ministerial Meeting, the United States and the European Union expressed their dedication to a risk-based strategy for AI and to promoting the development of AI systems that are safe, secure, and reliable. The TTC's devoted coordination is crucial for implementing policy measures that seek to maximise the advantages of AI while safeguarding persons and society from its potential threats, and ensuring the protection of human rights.[89]

[87] ISO/IEC 42001 Explained, supra note 57, at 34

[88] Ford, C., Nietsche, C., & Tar, J, *US-EU AI Code of Conduct: First Step Towards Transatlantic Pillar of Global AI Governance* (July 27, 2023), www.euractiv.com. https://www.euractiv.com/section/artificial-intelligence/opinion/us-eu-ai-code-of-conduct-first-step-towards-transatlantic-pillar-of-global-ai-governance/

[89] The White House, *U.S.-EU Joint Statement of the Trade and Technology Council*, (Apr. 5, 2024), https://www.whitehouse.gov/briefing-room/statements-releases/2024/04/05/u-s-eu-joint-statement-of-the-trade-and-technology-council-3/.

REGULATIONS BY SPECIFIC COUNTRIES

UNITED STATES OF AMERICA

The USA has undertaken comprehensive efforts to regulate and advance AI technologies, starting with strategic planning dating back to the Obama administration in 2016. These initiatives were built upon preceding White House reports focusing on big data and algorithmic systems. The National Science and Technology Council released the seminal "Preparing for the Future of Artificial Intelligence" whitepaper, providing recommendations for addressing fairness, safety, governance, and global security concerns.[90] Simultaneously, the National Artificial Intelligence Research and Development Strategic Plan outlined seven key strategies aimed at fostering AI research and development. This strategic plan underwent updates in 2019 and 2023 to further enhance its scope and effectiveness. The additional strategies emphasized expanding public-private partnerships and fostering international collaboration in AI research, reflecting the evolving landscape of AI technology. To streamline and coordinate these efforts, the National AI Initiative Office was established in 2021 under the National Artificial Intelligence Initiative Act of 2020.[91] This office is responsible for overseeing and implementing the national AI strategy, ensuring US leadership in developing and deploying trustworthy AI across various sectors.

Further, the Biden administration introduced the "Blueprint for an AI Bill of Rights" in 2022, outlining principles and core protections for the design and deployment of AI systems.[92] This blueprint was accompanied by federal actions aimed at protecting individuals' rights and safety while fostering AI development for the benefit of society. These principles aim to safeguard the American public from potential risks associated with the proliferation of automated systems and ensure that AI technologies are deployed in a manner consistent with fundamental values and rights. The Blueprint for an AI Bill of Rights, delineates five guiding principles intended to shape the design, implementation, and utilization of automated systems in alignment with the nation's highest ideals. These principles are Safety and Efficacy, Algorithmic Discrimination Protections, Data Privacy,

[90] Executive Office of the President National Science and Technology Council Committee on Technology, *Preparing For The Future of Artificial Intelligence* (2016)

[91] White House, Office of the Press Secretary, White House Launches National Artificial Intelligence Initiative Office (Nov. 19, 2018), archived at https://trumpwhitehouse.archives.gov/briefings-statements/white-house-launches-national-artificial-intelligence-initiative-office/

[92] White House, Office of Science and Technology Policy, AI Bill of Rights, (November 22, 2023) https://www.whitehouse.gov/ostp/ai-bill-of-rights/

Notice and Explanation and Human Alternatives, Consideration, and Fallback. The framework aims to ensure that such protections are applied consistently across various sectors, including civil rights, equal opportunities, and access to essential services.[93]

To facilitate public input and address emerging concerns, the White House Office of Science and Technology Policy issued a Request for Information to gather feedback on mitigating AI risks and harnessing its potential for societal improvement. Moreover, congressional hearings have been instrumental in guiding regulatory efforts and shaping AI policy. Topics of these hearings have ranged from intellectual property and human rights considerations to the oversight and management of AI risks. Additionally, on October 30, 2023, the White House released an Executive Order (EO) on AI, presenting the Biden administration's plan for promoting responsible AI advancement within the United States. This EO addresses various aspects, including safety protocols, privacy measures, fairness, innovation, and global leadership, and it represents a notable effort to bolster the country's stance in the field of AI. Nonetheless, the EO is constrained by its inability to enforce legal measures.[94]

While there is no comprehensive federal legislation, various sector-specific laws and pending federal and state regulations reflect the growing recognition of the need for governance in this area. Still there are case laws emerging on a daily basis which shows the requirement of a federal legislation. In the legal case Walters v. OpenAI (filed on June 5, 2023 in the Superior Court of Gwinnett County, Georgia)[95], it is claimed that OpenAI made defamatory statements against the Plaintiff. Fred Riehl, a journalist not affiliated with either party, utilized ChatGPT to aid in researching a legal matter. However, the information generated by ChatGPT contained fabricated accusations against the Plaintiff. Specifically, ChatGPT incorrectly described an ongoing lawsuit as accusing the Plaintiff of fraud and embezzlement, despite the Plaintiff not being involved in that particular case. One significant federal law is the Artificial Intelligence Training for the Acquisition Workforce Act (AI Training Act) of 2022.[96] This legislation mandates the Office of Management and

[93] Ibid.
[94] Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, The White House (Oct. 30, 2023), https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/
[95] Walters v. OpenAI LLC, No. 23-A-04860-2 (GA. Super. Ct. Jun 5, 2023)
[96] Artificial Intelligence Training for the Acquisition Workforce Act. (January 1, 2022). http://books.google.ie/books?id=GXgx0AEACAAJ&dq=ARTIFICIAL+INTELLIGENCE+TRAINING+FOR+THE+ACQUISITION+WORKFORCE+ACT&hl=&cd=1&source=gbs_api

Budget (OMB) to develop an AI training program to educate federal executive agencies about the capabilities and risks associated with AI technologies. The aim is to ensure informed procurement practices and awareness among individuals involved in acquiring AI. Furthermore, the National Defense Authorization Act 2023 (NDAA) directs defense and intelligence agencies to integrate AI systems into various operations, including intelligence collection, data management, and cybersecurity. The NDAA also emphasizes the need to develop recommendations and policies for federal AI use while assessing associated risks and impacts.[97] In the realm of consumer protection, existing federal laws such as Section 5 of the FTC Act,[98] the Fair Credit Reporting Act, and the Equal Credit Opportunity Act apply to specific applications of AI. These laws safeguard against discriminatory practices and ensure fairness in automated decision-making processes.

Federal agencies like the National Institute of Standards and Technology (NIST) have released guidance to manage AI-related risks effectively. The Artificial Intelligence Risk Management Framework 1.0 defines trustworthiness and provides implementation actions to mitigate risks, although adoption remains voluntary at present. Moreover, various federal agencies including the Consumer Financial Protection Bureau (CFPB), the Department of Justice's Civil Rights Division, the Equal Employment Opportunity Commission (EEOC), and the Federal Trade Commission (FTC) enforce civil rights, non-discrimination, fair competition, and consumer protection concerning AI applications. For instance, the CFPB has issued guidance on the application of the Equal Credit Opportunity Act to algorithmic credit decisions, emphasizing transparency and accountability.[99]

At the state level, numerous laws have been enacted to address AI-related issues, such as consumer discrimination in insurance practices and privacy concerns. States like California, Colorado, Connecticut, Illinois, Maryland, Montana, New York, Tennessee, Texas, and Virginia have introduced legislation covering various aspects of AI governance,

[97] The White House, Statement by the President on H.R. 7776, the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, (December 23, 2022) https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/23/statement-by-the-president-on-h-r-7776-the-james-m-inhofe-national-defense-authorization-act-for-fiscal-year-2023/

[98] Section 5 of the Federal Trade Commission Act (FTC Act) (15 USC 45) prohibits "unfair or deceptive acts or practices in or affecting commerce." The FTC has issued a number of guidance documents and engaged in enforcement activity demonstrating what it believes to be deceptive or unfair when businesses use these tools. Businesses that do not follow this guidance face investigation and potential enforcement, with the FTC coming up with creative penalties designed to dissuade improper behaviour, including the disgorgement of algorithms, data, and other inputs to and outputs of unlawful AI systems.

[99] Federal Trade Commission, Equal Credit Opportunity Act, (April 3, 2024) https://www.ftc.gov/legal-library/browse/statutes/equal-credit-opportunity-act

including data protection, privacy rights, and transparency requirements. Additionally, both federal and state legislatures have proposed several bills and frameworks to further regulate AI. For instance, proposed federal legislation includes the SAFE Innovation Framework, the National AI Commission Act, and the Algorithmic Accountability Act, which seek to establish comprehensive regulatory frameworks and promote responsible AI development. In a case against Workday, it was alleged that their AI systems, utilizing algorithms and human-generated inputs, unfairly disadvantage Black individuals, disabled persons, and older job seekers, potentially leading to their exclusion from employment opportunities.[100] Another lawsuit, involving State Farm Fire & Casualty Company, contends that the algorithms and analytical tools employed by State Farm exhibit biased tendencies in data analysis. These cases highlight growing concerns over the discriminatory impacts of AI technologies in hiring practices and data interpretation within corporate environments.[101]

In conclusion, while the United States lacks a federal AI regulation comparable to the European Union AI Act, it has made significant strides in regulating AI through existing laws, sector-specific regulations, and ongoing legislative efforts at both the federal and state levels. In essence, these multifaceted initiatives underscore the USA's commitment to fostering responsible AI development while addressing ethical, legal, and societal implications, ensuring that AI technologies serve the interests of individuals and society as a whole.

UNITED ARAB EMIRATES

In 2017, the UAE initiated significant steps towards regulating AI with the appointment of H.E. Omar Bin Sultan Al Olama as the Minister of State for Artificial Intelligence. Following this, in April 2019, the UAE Cabinet sanctioned the National Strategy for Artificial Intelligence 2031, aiming to position the UAE as a global leader in AI technologies. This strategy was accompanied by the establishment of the Office of Artificial Intelligence to oversee its implementation. The UAE Artificial Intelligence and Blockchain Council (the "Council") was subsequently appointed by the UAE Cabinet to supervise the integration of AI technologies across society and government sectors. Tasked with proposing

[100] Mobley v. Workday, Inc., 3:23-cv-00770, (N.D. Cal.)
[101] *Huskey v. State Farm Fire & Cas. Co.*, 22 C 7014 (N.D. Ill. Sep. 11, 2023)

policies conducive to an AI-friendly ecosystem while upholding privacy and ethical standards, the Council plays a pivotal role in shaping the regulatory landscape.[102]

A pivotal initiative in this regulatory framework is the UAE Regulations Lab (RegLab), established in January 2019. The RegLab operates proactively to anticipate and formulate legislation governing the use of emerging technologies, including AI. It serves as a platform for granting temporary licenses for testing and vetting innovative AI-driven solutions. Furthermore, within free zones like the Abu Dhabi Global Market (ADGM) and the Dubai International Financial Centre (DIFC), specialized programs such as the ADGM RegLab and the DIFC Innovation Testing License (ITL) Programme offer a controlled environment for testing fintech innovations, mitigating regulatory barriers. Moreover, regulatory bodies such as the Central Bank of the UAE and financial authorities in free zones have issued guidelines for financial institutions adopting enabling technologies, including AI. Although these guidelines are currently in a draft stage, they underscore the necessity for robust governance, accountability, and consumer protection frameworks concerning AI applications in financial services.[103]

In terms of legal principles, the UAE's civil law framework, encompassing laws such as the Civil Transaction Law, Consumer Protection Law, and Product Safety Law, provides the foundation for regulating AI. Notably, Article 316 of the Civil Code establishes liability for individuals overseeing potentially harmful entities or mechanical equipment, which could extend to AI-powered systems. However, attributing liability in AI-related incidents presents challenges due to the distributed nature of responsibility, involving engineers, funding entities, and deploying organizations. Addressing criminal liability, Federal Decree Law No. 31 of 2021 outlines the elements of criminal acts, emphasizing both actus reus (the physical act) and mens rea (the intent or fault). While the mere use of AI does not constitute criminal activity, defining and categorizing AI applications to determine potential criminal acts remains a key challenge for legislators. The UAE has taken significant strides in regulating AI through the establishment of specialized bodies, proactive legislative initiatives, and the integration of AI considerations into existing legal frameworks. However,

[102] Artificial Intelligence Council, Government of the United Arab Emirates, accessed on January 16, 2024, https://ai.gov.ae/ai_council/

[103] UAE Government, *National Program for Artificial Intelligence*, https://ai.gov.ae/wp-content/uploads/2020/02/AIGuide_EN_v1-online.pdf

navigating the complexities of AI regulation, particularly concerning liability and criminality, remains an ongoing endeavour for policymakers and legal experts alike.

PEOPLE’S REPUBLIC OF CHINA

China has placed significant emphasis on advancing its AI industry, elevating it to a national strategic priority. In a landmark move in July 2017, the central government unveiled the New Generation Development Plan for Artificial Intelligence, marking the inaugural systematic blueprint for nationwide AI industry development. Recognizing AI's pivotal role as an emerging economic catalyst, the plan underscored the imperative for robust institutional frameworks at the national level.[104] This encompassed the enactment of AI-related legislation, regulatory frameworks, ethical guidelines, safety monitoring systems, and the establishment of technical standards and intellectual property rights mechanisms. China has implemented three significant regulations concerning algorithms and AI: the 2021 regulation pertaining to recommendation algorithms, the 2022 rules addressing deep synthesis or synthetically generated content, and the 2023 draft regulations regarding generative AI. While these regulations primarily aim at controlling information, they encompass various noteworthy provisions. For instance, the rules regarding recommendation algorithms aim to prevent excessive price discrimination and safeguard the rights of workers subjected to algorithmic scheduling. Similarly, the deep synthesis regulation mandates the prominent labelling of synthetically generated content. Additionally, the draft generative AI regulation necessitates both the training data and model outputs to be "true and accurate,” presenting a considerable challenge for AI chatbots. All three regulations mandate developers to register with China's algorithm registry, a newly established government database collecting information on algorithm training, and necessitate them to undergo a security self-assessment.[105] In a case known as Guo Bing vs. Hangzhou Wildlife World Service Contract Dispute[106], the court acknowledged that biometric data qualifies as sensitive personal information. It ruled that operators may only gather and utilize such data with the explicit consent of consumers, adhering strictly to the principles of legality, legitimacy, and necessity. The unilateral switch by the operator from

[104] Full Translation: China’s “New Generation Artificial Intelligence Development Plan” (2017) - DigiChina. (October 1, 2021), https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/

[105] Franks, E., Lee, B., & Xu, H.. *Report: China’s New AI Regulations*, Global Privacy Law Review, 5 (Issue 1), 43–49 (March 1, 2024), https://doi.org/10.54648/gplr2024007

[106] Guo Bing vs. Hangzhou Wildlife World Service Contract Dispute, Zhe Jiang 0111 Min Chu No. 6971((2019), Commonly known as the First Facial Recognition Dispute.

fingerprint recognition to facial recognition was deemed a violation of the contract terms. Consequently, consumers were entitled to demand the removal of any personal information associated with this breach.

Presently, China is in the midst of transitioning its legal landscape for AI, shifting from a focus on addressing immediate needs to constructing a comprehensive regulatory framework. The Artificial Intelligence Law has been slated for inclusion in the legislative agenda. The current regulatory landscape primarily hinges on specialized legislation targeting key sectors and critical issues in AI applications. In the realm of cybersecurity and data protection, China has leveraged existing legal frameworks such as the Cybersecurity Law, Data Security Law, and the forthcoming Personal Information Protection Law. Additionally, specialized regulations have been crafted to address high-risk AI applications. For instance, the Administrative Provisions on Recommendation Algorithms in Internet-based Information Services delineate guidelines encompassing information security management, user rights protection, and the mandatory filing of algorithms by providers with regulatory authorities. These regulations represent foundational governance structures for AI and algorithmic oversight in China.[107]

Similarly, the Administrative Provisions on Deep Synthesis in Internet-based Information Services specifically target deep synthesis technologies like Deepfake, outlining provisions for information security accountability and content labelling. Moreover, the Provisional Measures for the Administration of Generative Artificial Intelligence Services focus on regulating model applications such as ChatGPT, setting forth requirements for training data processing legitimacy and operational management. Ethical considerations are also integral to China's AI regulatory framework, with dedicated efforts to establish ethical norms. The Measures for Ethical Review of Science and Technology (Trial Implementation) highlight AI as a subject for ethical scrutiny, outlining procedures and standards for ethical review. Likewise, the Ethical Guidelines for Next-Generation Artificial Intelligence delineate fundamental ethical norms governing various AI activities, spanning management, research, development, and utilization.[108]

[107] Legal 500, China: Artificial Intelligence, https://www.legal500.com/guides/chapter/china-artificial-intelligence/?_gl=1*1xn67w8*_up*MQ..*_ga*MTYzOTkxNDYyNS4xNzE0MTY5MjA0*_ga_JFNJC5V947*MTcxNDE2OTIwMy4xLjAuMTcxNDE2OTIwMy4wLjAuMA (last visited April 24, 2024).

[108] Briefing, C., *Ethics in China: Trial Measures for Ethical Review of Science & Technology*, China Briefing News, (May 17, 2023). https://www.china-briefing.com/news/china-ethical-review-of-science-and-technology-draft-trial-measures/

Despite advancements in regulatory frameworks, China's approach to civil liability for AI-related harm remains nascent. Damages stemming from AI systems generally fall under traditional tort laws, with principles of fault liability applied in most cases. However, specific tort rules may be invoked in specialized areas like product liability, motor vehicle accidents, and medical malpractice. China has yet to establish dedicated criminal statutes targeting AI-induced harm. However, ongoing regulatory developments underscore the nation's commitment to enhancing AI governance across diverse domains.

JAPAN

There is currently no legislation or regulation specific to AI in Japan. Under Japanese law, the laws generally applicable to AI are the Civil Code, the Product Liability Law, and the Penal Code. In April 2022, Japan took significant strides in regulating AI with the publication of the "AI Strategy 2022" by the Cabinet Office's Integrated Innovation Strategy Promotion Council. This strategy aimed to provide comprehensive guidance on the nation's AI initiatives. Building upon this, in April 2023, the Liberal Democratic Party of Japan's (LDP) Digital Society Promotion Headquarters released the "AI White Paper: Japan's National Strategy in the New Era of AI."[109] Recognizing the profound impact of large language models (LLMs), such as ChatGPT, on society, this white paper underscored the necessity for a revamped national strategy to navigate this evolving landscape. To spearhead this effort, Japan established the AI Strategic Council and the AI Strategic Team in May and April 2023, respectively. These bodies were entrusted with formulating a cohesive national approach to AI. Moreover, during the G7 Hiroshima Summit in May 2023, Japan convened discussions among G7 leaders regarding general AI usage. An agreement was reached to consolidate perspectives on crucial aspects like copyright protection and misinformation combat, aiming to craft international regulations by year-end.

Currently, Japan has implemented various rules and guidelines governing AI, encompassing issues ranging from summarizing AI concerns to conducting in-depth investigations into AI implementation and operation challenges. These include the "Tentative Summary of AI Issues," "AI Strategy 2022," "AI White Paper: Japan's National Strategy in the New Era of AI," "Governance Guidelines for Implementation of AI Principles Ver. 1.1," "AI Utilization Guidelines Practical Reference for AI Utilization," "Social

[109] LDP Headquarters for the Promotion of Digital Society Project Team on the Evolution and Implementation of Ais, *The AI White Paper Japan's National Strategy in the New Era of AI*, April 2023, https://www.taira-m.jp/ldp%E2%80%99s%20ai%20whitepaper_etrans_2304.pdf

Principles of Human-Centric AI," and "Draft AI R&D GUIDELINES for International Discussions." These regulatory frameworks collectively reflect Japan's proactive stance in addressing the multifaceted dimensions of AI governance.[110]

CANADA

Canada has taken significant steps to regulate the burgeoning field of AI through a series of legislative measures and policy initiatives. The cornerstone of these efforts is Canada's "Digital Charter", which was unveiled by the federal government in 2019. Embedded within this charter is the "Pan-Canadian AI Strategy", structured around three key pillars to foster innovation, set standards, and attract talent in the AI sector. Firstly, the strategy includes substantial financial backing for three national AI institutes and five innovation clusters, facilitating the commercialization of AI technologies. Secondly, it provides support to the Standards Council of Canada for the development of standards specific to AI, ensuring ethical and technical guidelines are in place. Thirdly, it invests in academic training and research centres alongside organizations offering computational resources tailored for AI research to nurture and retain AI talent within Canada.[111] In July 2021, the federal government initiated the Consultation on Modern Copyright Framework for Artificial Intelligence and the Internet of Things (IoT), seeking input to adapt copyright policies to the challenges posed by AI. While the consultation gathered feedback from various stakeholders, subsequent steps have yet to be announced by the government. In the case of Haghshenas v Canada[112], the Federal Court reviewed the use of artificial intelligence in administrative decision-making. The case involved a judicial review of a decision by a Canadian immigration officer who had denied a work permit application based on information processed by an AI system named Chinook. The court determined that the decision was procedurally fair because it was ultimately made by the immigration officer, not the AI system. Additionally, the court dismissed the argument that using the AI system made the decision substantively unreasonable. Also, in Orpheus Medica v Deep Biologics Inc.[113], the plaintiff sought a preliminary injunction against former employees accused of

[110] Legal 500, Japan: Artificial Intelligence, https://www.legal500.com/guides/chapter/japan-artificial-intelligence/?_gl=1*1yutmji*_up*MQ..*_ga*NDExNjUwNDk5LjE3MTQxNjk1MDI.*_ga_JFNJC5V947*MTcxNDE2OTUwMi4xLjAuMTcxNDE2OTUwMi4wLjAuMA

[111] Canada, Innovation, Science and Economic Development Canada, *Canada's Digital Charter: Trust in a Digital World,* Innovation, Science and Economic Development Canada, https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter-trust-digital-world

[112] Haghshenas v Canada (Citizenship and Immigration) 2023 FC 464

[113] Orpheus Medica v Deep Biologics Inc, 2020 ONSC 4974

misappropriating confidential information. The plaintiff argued that the stolen information included their method of using AI to analyze a database of certain antibodies. The Ontario Superior Court of Justice denied the motion, ruling that the use of AI for such purposes was neither unique nor confidential to the plaintiff. Furthermore, the AI system in question was not proprietary, as the plaintiff used publicly available open-source programs.

One significant legislative proposal introduced by the Canadian federal government is Bill C-27, aimed at modernizing the Personal Information Protection and Electronic Documents Act (PIPEDA) and introducing the Artificial Intelligence and Data Act (AIDA). Under AIDA, a principles-based approach is advocated to govern AI usage, focusing on preventing harm to individuals, property damage, and economic loss, particularly by addressing biases in AI outputs. AIDA targets "high-impact" AI systems and imposes obligations on developers, providers, and managers to ensure compliance with its provisions.[114] Notably, it places responsibility on those involved in international or interprovincial trade and commerce to identify, assess, and mitigate risks associated with AI systems. Furthermore, AIDA mandates measures for anonymizing and managing data used by regulated activities. While AIDA's current form is relatively basic, leaving detailed regulations for subsequent enactment, it establishes a framework for monitoring and penalizing non-compliance, with potential penalties of up to $10 million CAD or 3% of global annual revenues for offences. Thus, AIDA aims to provide a regulatory framework that balances innovation with accountability in Canada's rapidly evolving landscape of AI technology.[115] In the case of James v Amazon.com.ca, Inc.[116], the Federal Court rejected the applicant's request for a declaration that the respondent's AI-based automated data request decision-making process violated the PIPEDA. The court dismissed the application because the requested relief exceeded the scope of the applicant’s original complaint to the OPC, the issue had not been addressed by the OPC in its investigation, and there was no basis in the record to consider the claim.

UNITED KINGDOM

In September 2021, the UK government introduced its National AI Strategy, envisioning the nation as a "global AI superpower" within the next decade. The primary goal

[114] Cassels. *The Landscape of AI Regulation in Canada,* Cassels (February 11, 2024), https://cassels.com/insights/the-landscape-of-ai-regulation-in-canada/.
[115] Legal 500, Canada: Artificial Intelligence, available at https://www.legal500.com/guides/chapter/canada-artificial-intelligence/
[116] James v Amazon.com.ca, Inc., 2023 FC 166

is to harness AI's potential for fostering growth, prosperity, and societal benefits. Although the strategy lacks specifics on forthcoming legal principles or statutory frameworks, it aims to invest in the AI ecosystem's long-term needs, facilitate the transition to an AI-driven economy, and ensure appropriate national and international governance of AI technologies. Emphasizing the importance of public trust and diverse societal input, the strategy underscores the significance of broad societal engagement.[117]

Subsequently, in July 2022, the UK unveiled its AI Action Plan, outlining further initiatives to advance the National AI Strategy. In March 2023, the UK government issued a White Paper titled "A pro-innovation approach to AI regulation," acknowledging the absence of a universally accepted definition of AI. Instead, the government delineated AI based on two key characteristics: adaptivity and autonomy. Notably, the UK has yet to enact clear standalone regulations or guidelines for AI. However, the March 2023 White Paper proposed a regulatory framework characterized as pro-innovation, proportionate, trustworthy, adaptable, clear, and collaborative. A consultation on this White Paper concluded in June 2023.

The White Paper introduced five values-focused cross-sectoral principles to guide regulators in implementing AI regulation. These principles prioritize safety, security, and robustness; appropriate transparency and explainability; fairness; accountability and governance; and contestability and redress. While these principles are intended to steer responsible AI development and usage, it's important to note that the White Paper primarily serves as a policy document and does not establish binding rules or detailed guidelines on AI regulation.[118] Despite this, the UK government has not signalled imminent plans for specific AI legislation. Current AI regulation in the UK primarily relies on existing legal frameworks, such as data protection laws and intellectual property principles. Additionally, several indicative standards, including the AI Standards Hub and the Responsible Machine Learning Principles, shape AI deployment practices within the country.[119] The case of Stephen Thaler v. Comptroller-General of Patents, Designs and Trade Marks[120] which was

[117] National AI Strategy - HTML version. (2022, December 18). GOV.UK. https://www.gov.uk/government/publications/national-ai-strategy/national-ai-strategy-html-version
[118] UK Government, Department for Digital, Culture, Media & Sport, *A Pro-Innovation Approach to AI Regulation*, https://assets.publishing.service.gov.uk/media/64cb71a547915a00142a91c4/a-pro-innovation-approach-to-ai-regulation-amended-web-ready.pdf
[119] Legal 500, United Kingdom: Artificial Intelligence, https://www.legal500.com/guides/chapter/united-kingdom-artificial-intelligence/
[120] Stephen Thaler v. Comptroller-General of Patents, Designs and Trade Marks (2023, UKSC 49)

one of the highlighted case laws emerged relating to Artificial Intelligence involves the attempt to register patents for inventions created by the Al system 'DABUS.' Dr. Stephen Thaler, the creator of DABUS, claimed that the Al system should be recognized as the inventor. The Supreme Court, led by Lord Kitchin, dismissed the appeal, affirming that under the 1977 Act, an inventor must be a natural person, and machines like DABUS do not qualify as inventors. The court further clarified that Dr. Thaler had no right to secure patents for the inventions described in the applications, as DABUS lacked legal personality. The decision raises challenges in addressing the ownership and protection of Al-generated innovations under current intellectual property laws.

On February 6, 2024, the UK Government issued its long-awaited response to the previous year's White Paper consultation on AI regulation. The response largely maintains the initial "pro-innovation" stance and outlines a principles-based, non-statutory, cross-sector framework. The objective is to strike a balance between fostering innovation and ensuring safety by applying existing technology-neutral regulatory structures to AI. While acknowledging the necessity of future legislative action, particularly concerning General-Purpose AI systems, the UK deems it premature to enact such measures. Instead, it emphasizes the importance of understanding AI's risks, challenges, and regulatory gaps before pursuing legislative interventions. This approach diverges from that of other jurisdictions, such as the EU and, to some extent, the US, which are adopting more prescriptive legislative measures. Despite international cooperation agreements, the contrasting approaches underscore the potential for regulatory divergence in the global AI landscape.

INDIA

India is still grappling with its policies and their application to AI. The country's courts have yet to rule on the legal status of AI and the relevant laws. Despite this uncertainty, certain protections are in place for specific uses of AI. The Copyright Act, 1957, under section 2(o), classifies the source or object code of AI applications as Literary work, thus granting the developer ownership of their work under copyright protection. However, per section 3(k) of the Patents Act, 1970, computer programs alone are not patentable unless they are part of a hardware-software invention. In India, AI applications' design, idea, and structure are also safeguarded as Trade Secrets under Contract and Tort laws, with access provided through License Agreements that include 'exclusive license' provisions to manage and defend intellectual property rights. Despite these protections, intellectual property generated by AI itself is not recognized as the machine cannot be the owner, as affirmed in Rupendra Kashyap v. Jiwan Publishing House Pvt. Ltd.,[121] where it was ruled that copyright belongs only to natural persons. Personal data within big data is protected under the Information Technology Act, 2000, and the 'right to privacy' under Article 21 of the Indian Constitution. The rise of AI and big data has positioned many enterprises advantageously to predict consumer behaviour and enhance efficiency but has also led to concerns about anti-competitive practices. For instance, in Delhi Vyapar Mahasangh v. Flipkart Internet Pvt. Ltd. and Amazon Seller Services[122], it was noted that AI-enabled data analysis by Amazon and Flipkart marginalized competitors, prompting an investigation by the Competition Commission of India. Section 6(1) of the Competition Law empowers the Commission to address market impacts, and although specific AI-related regulations are lacking, sections 20 and 3 of the Competition Act, 2020, can be applied to deem collusive arrangements as anti-competitive.

In 2018, NITI Aayog introduced India's inaugural national AI strategy, titled #AIFORALL, which aimed to adopt an inclusive approach to artificial intelligence. This strategy highlighted key sectors for AI innovation and application, such as healthcare, education, agriculture, smart cities, and transportation. Since its launch, several recommendations have been implemented, including the development of high-quality datasets to foster research and innovation, and the establishment of legislative frameworks for data protection and cybersecurity. In February 2021, NITI Aayog formulated the Principles for Responsible AI, building on the National Artificial Intelligence Strategy. This document addresses ethical considerations in AI deployment in India, divided into system and societal concerns. System considerations cover decision-making principles, fair beneficiary inclusion, and accountability, while societal considerations focus on the impact of automation on employment.[123] The paper delineates seven core principles for the responsible governance of AI systems: safety and reliability, inclusivity and non-discrimination, equality, privacy and security, transparency, accountability, and the reinforcement of positive human values. In August 2021, NITI Aayog released the second

[121] Rupendra Kashyap v. Jiwan Publishing House Pvt. Ltd 1996 38 DRJ 81

[122] Delhi Vyapar Mahasangh v. Flipkart Internet Pvt. Ltd. And Amazon Seller Services Case no. 40 of 2019 [Order 13.01.2020]

[123] NITI Aayog, *National Strategy for Artificial Intelligence*, NITI Aayog, Gov't of India (Mar. 2023), https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf.

part of the principles for responsible AI, which emphasizes the practical application of these ethical guidelines.[124] This document stresses the importance of government involvement in fostering responsible AI use in social sectors, collaborating with the private sector and research institutions. It highlights the need for regulatory and policy measures, capacity building, and promoting ethical practices among private entities involved in AI.[125]

The Digital Personal Data Protection Act, 2023, was enacted by the President of India on August 11, 2023. This Act, effective immediately, regulates the processing of digital personal data in India, addressing some of the privacy concerns associated with AI platforms.[126] The IT Rules 2021, issued by the Government of India under the Information Technology Act of 2000, provide a framework for regulating entities such as social media intermediaries, OTT platforms, and digital news media. These rules were implemented on May 26, 2021, and updated on April 6, 2023. On May 26, 2022, MeitY released the draft National Data Governance Framework Policy (NDGFP). This policy aims to modernize and improve government data collection and management. The NDGFP's primary goal is to create an ecosystem that supports AI and data-driven research and startups in India by establishing a comprehensive dataset repository. The Ministry of Electronics and Information Technology has formed committees on AI to provide reports on AI development, safety, and ethical issues. Similarly, the Bureau of Indian Standards, India's national standards body, has created a committee dedicated to AI, which is working on drafting Indian standards for the field.

Deepfakes, which are digitally altered media created using AI, can damage reputations, fabricate evidence, and undermine trust in institutions. Current legislation provides civil and criminal remedies for such offenses. For example, Section 66E of the Information Technology Act, 2000, addresses privacy violations by deepfakes, with penalties including imprisonment up to three years or fines up to INR 200,000. Section 66D covers the malicious use of communication devices or computer resources, also punishable by imprisonment and/or fines. Additionally, Sections 67, 67A, and 67B of the IT Act address

[124] NITI Aayog, *Responsible AI for All: Adopting the Framework – A Time for Action*, (Feb. 2021), https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf
[125] NITI Aayog, *Responsible AI for All: Part 2*, (2021), available at https://www.niti.gov.in/sites/default/files/2021-08/Part2-Responsible-AI-12082021.pdf.
[126] Data Protection Law Hub, *India Pushes Ahead with New Digital Personal Data Protection Act*, (June 14, 2023), https://dataprotectionlawhub.com/blog/india-pushes-ahead-new-digital-personal-data-protection-act.

the publication or transmission of obscene deepfakes, requiring social media platforms to remove such content promptly or risk losing 'safe harbour' protection.[127]

The Indian Penal Code also offers recourse for deepfake-related cybercrimes under Sections 509 (insulting the modesty of a woman), Section 499 (criminal defamation), and Section 153(a) and (b) (spreading hate on communal lines), among others. Recent cases show law enforcement applying forgery-related sections in deepfake incidents. On March 15, 2024, MeitY issued a new advisory, superseding the previous advisory from March 1, 2024. This advisory must be read alongside the one from December 26, 2023, and addresses concerns about intermediaries and platforms neglecting due diligence obligations as outlined in the IT Rules 2021.

CONCLUSION

The chapter has analysed various global attempts to govern AI, ranging from international entities to individual nations. Nevertheless, it is clear that none of these efforts have yielded definitive or adaptable results. So far, they have not been able to demonstrate true effectiveness or efficiency in controlling the constantly changing field of AI development. The current legal frameworks have challenges in effectively addressing the complex technology encompassed by today's AI. This underscores the necessity for a more thorough and standardised regulation of AI in order to successfully address the intricate difficulties presented by this advanced technology. Although world leaders from the United States, United Kingdom, China, and other countries expressed strong support for regulating AI, none of them were willing to take the bold step of actually implementing strict regulations for this rapidly advancing technology. The focus is on establishing effective management of AI without imposing excessive limitations, in order to promote ongoing advancements in the field. Even Sam Altman, the CEO of ChatGPT, acknowledged the necessity of regulation. But the European Union was determined enough to be first ones to regulate AI.

[127] India Briefing, *India: Regulation of AI and Large Language Models*, INDIA BRIEFING (June 13, 2024), https://www.india-briefing.com/news/india-regulation-of-ai-and-large-language-models-31680.html.

CHAPTER 4

THE EUROPEAN UNION'S ARTIFICIAL INTELLIGENCE ACT- A COMPREHENSIVE OVERVIEW

INTRODUCTION

AI has emerged as a key focus in the European Union's strategy for regulating digital technologies. The European Commission has consistently emphasised the need of promoting the implementation of AI technologies in the EU through legislative amendments, including those related to the EU data protection framework. Policies targeting several aspects of the European digital single market also encompassed rules specifically addressing AI. In March 2021, the Commission introduced a strategic roadmap for the Digital Decade, anchored by the 2030 Digital Compass—a blueprint designed to steer the European Union towards comprehensive digital evolution across its economy and society.[128] The Digital Compass sets its sights on cultivating a secure digital environment centred around human needs, fostering citizen empowerment, and facilitating business growth through digital opportunities. It delineates four key focal points to guide this journey: enhancing digital skills, establishing resilient and efficient digital infrastructure, facilitating digital adaptation for businesses, and promoting the digitization of public services. This agenda underscores adherence to EU standards and norms to fortify the Union's digital autonomy, with various financial instruments earmarked to support the requisite investments for laying the groundwork for Europe's digital transformation over the next decade.[129] A series of legislations and regulations were made as part of this agenda. After the enactment of the Digital Market and Digital Services Acts in 2022,[130] the AI Act marks the final technological legislation approved during the tenure of the European Parliament and Commission spanning from 2019 to 2024. This legislative series aligns with the above-said overarching

[128] Digital Decade Policy Programme, Government of Luxembourg. https://gouvernement.lu/en/dossiers.gouv_smc%2Ben%2Bdossiers%2Bdigital-decade1%2Bdigital-decade.html#:~:text=The%20Digital%20Decade%20policy%20programme,Europe’s%20digital%20transformation%20by%202030.

[129] European Commission, Europe Fit for the Digital Age, Europe's Digital Decade: Digital Targets 2023, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030-un

[130] European Commission, Digital Strategy, Digital Services Act Package, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

goal of fostering a digitally progressive Europe, combining heightened scrutiny of technology with endeavours aimed at pioneering digital policy-making.

The European Parliament, on 13th March 2024, overwhelmingly passed the European Union Artificial Intelligence Act or AI Act, which had been introduced by the European Commission in April 2021. This Act marks the first globally applicable regulation on AI, establishing a unified framework governing the utilization and distribution of AI systems within the EU. It introduces a classification system for AI systems, with varying requirements and responsibilities determined by a 'risk-based approach'. Prohibited are AI systems deemed to present 'unacceptable' risks, while a set of prerequisites and responsibilities are mandated for 'high-risk' AI systems, which could potentially endanger individuals' health, safety, or fundamental rights. Additionally, AI systems categorized as posing limited risks due to transparency concerns will be subject to information and transparency stipulations, while those presenting minimal risks will not face further obligations. Specific provisions are outlined for General Purpose AI (GPAI) models, with more stringent requirements imposed on GPAI models deemed to have 'high-impact capabilities', potentially posing systemic risks to the internal market.[131]

LEGISLATIVE FRAMEWORK OF THE AI ACT

The AI Act was shaped by the European Union’s ordinary legislative procedure, the process by which most EU legislations are produced. It is important to point out the most significant developments in the legislative process to understand the amount of time and effort spent in developing this law. The process technically commenced when the European Commission published a proposal to regulate artificial intelligence in the European Union on April 21st 2021. Then on July 20th, the Slovenian Presidency of the Council of the European Union organized a virtual conference on the regulation of artificial intelligence, ethics, and fundamental rights. Subsequently, a study analyzing the use of biometric techniques from an ethical and legal perspective commissioned by the European Parliament’s Policy Department for Citizens’ Rights and Constitutional Affairs was published, coinciding with the end of the public consultation period on the AI Act by the European Commission, which received 304 submissions. Later on February 2nd 2022, the European Commission presented a new Standardization Strategy outlining their approach to

[131] Yan, B. (n.d.), *EU passes landmark AI law*, Scot Scoop News, https://scotscoop.com/eu-passes-landmark-ai-law/#:~:text=On%20March%2013%2C%20the%20European,in%20favor%20to%2046%20against.

standards within the Single Market as well as globally, emphasizing their role in the EU Single Market and global competitiveness. On May 25th, the lead committees of the European Parliament, the Internal Market, and Civil Liberties committees, had their first joint exchange of views on the AI Act proposal. The year 2022 also saw significant legislative progress with key events such as the circulation of a compromise text of Articles 16-29 and Articles 40-52 of the proposed AI Act by the French Presidency of the Council. Fast forward to 2023, on June 14th, the European Parliament adopted its negotiating position on the AI Act. On December 9th of the same year, the Parliament and the Council reached a provisional agreement on the AI Act. In 2024, the European Union's member states unanimously endorsed the AI Act on February 13th, followed by the launch of the European Artificial Intelligence Office on February 21st to support the implementation of the AI Act. Finally, on 13th March 2024, the EU parliament, with 523 votes in favour to 46 against, passed the first-ever binding artificial intelligence regulation in history, the Artificial Intelligence Act. After some more procedural compliances, the Act will most likely become law by the end of June this year.[132]

OVERVIEW OF THE ACT

The AI Act basically defines AI and the contents are organised around the risk classification of AI technologies. It delineates unacceptable risks, such as social scoring systems and manipulative AI, which are strictly prohibited. The Act predominantly focuses on regulating high-risk AI systems, with a smaller segment addressing limited-risk AI systems. The latter category entails lighter transparency obligations, mandating developers and deployers to ensure end-users are informed when interacting with AI technologies like chatbots and deepfakes. Meanwhile, AI applications categorized as minimal risk remain unregulated, encompassing various everyday applications like AI-enabled video games and spam filters, albeit subject to change, especially concerning generative AI. The Act primarily imposes obligations on providers (developers) of high-risk AI systems, irrespective of their geographic location. This encompasses entities intending to introduce high-risk AI systems into the EU market, including those based outside the EU whose AI outputs are utilized within the EU.[133]

[132] Timeline of Developments | EU Artificial Intelligence Act. (n.d.). https://artificialintelligenceact.eu/developments/

[133] EU Artificial Intelligence Act | Up-to-date developments and analyses of the EU AI Act. (n.d.). https://artificialintelligenceact.eu/

The Act distinguishes between users deploying AI systems in a professional capacity and end-users directly affected by the technology. Users, typically organizations or individuals utilizing AI professionally, bear some obligations but to a lesser extent than providers. These obligations apply to users within the EU and those outside the EU whose AI systems impact the EU. Regarding GPAI, providers of GPAI models are required to furnish technical documentation and usage instructions and comply with copyright directives. Additionally, they must publish a summary of the training data employed. While providers offering free and open-license GPAI models have fewer obligations, they must still adhere to copyright regulations and disclose training data summaries unless posing systemic risks. Providers of GPAI models deemed to pose systemic risks, regardless of their openness or closure, are further obligated to conduct model evaluations, adversarial testing, report serious incidents, and ensure cybersecurity measures are in place.[134]

CONTENTS OF THE ACT

The AI Act consists of 113 Articles grouped into 13 Chapters. It also contains 13 annexes attached to the final draft.[135] Additionally, the Annexes accompanying the Act offer supplementary information regarding the regulation. The titles and the articles which come under each title are:

- Chapter I: General Provisions

Under this chapter, Articles 1 to 3 define the subject matter, scope, and key definitions relevant to AI technologies. Article 4 introduces the concept of AI literacy, emphasizing the importance of understanding AI systems by taking proper measures by providers and developers.[136]

- Chapter II: Prohibited Artificial Intelligence Practices

The single article, Article 5, enumerates specific practices that are prohibited under this regulation, safeguarding against potential risks associated with AI deployment.[137]

[134] EU Parliament, Artificial Intelligence Act, (March 13, 2024),. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

[135] The AI Act Explorer, EU Artificial Intelligence Act. (n.d.). https://artificialintelligenceact.eu/ai-act-explorer/

[136] EU Artificial Intelligence Act. (n.d.)., Chapter I: General Provisions https://artificialintelligenceact.eu/chapter/1/

[137] EU Artificial Intelligence Act. (n.d.)., Chapter II: Prohibited Artificial Intelligence Practices https://artificialintelligenceact.eu/chapter/2/

- Chapter III: High-Risk AI Systems

This chapter addresses the classification and regulation of high-risk AI systems, aiming to mitigate potential hazards associated with their deployment. This chapter is subdivided into 5 sections:

- Section 1: Classification of AI Systems as High-Risk
  This section outlines guidelines for categorizing AI systems as high-risk. Articles 6 and 7 specify the criteria for classification and the procedure for amending classifications, ensuring a uniform and consistent classification of high-risk AI systems.
- Section 2: Requirements for High-Risk AI Systems
  This section outlines stringent requirements for developing, deploying, and managing high-risk AI systems. Articles 8 to 15 specify compliance measures, risk management protocols, data governance standards, technical documentation and the necessity of human oversight to ensure the safety and reliability of these systems.
- Section 3: Obligations of Providers and Deployers of High-Risk AI Systems and Other Parties
  This section imposes obligations on providers, deployers, and other stakeholders involved in the lifecycle of high-risk AI systems. Articles 16 to 27 talks about responsibilities regarding quality management, documentation, transparency, obligations of deployers and distributors, cooperation with authorities, and fundamental rights impact assessments.
- Section 4: Notifying Authorities and Notified Bodies
  This section imposes the requirement for establishing at least one notifying authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring. Articles 28 to 39 outline the notification procedure, requirements for notified bodies, subsidiaries of and subcontracting by notified bodies, conformity assessment procedures, and coordination mechanisms of notified bodies.
- Section 5: Standards, Conformity Assessment, Certificates, Registration
  This section provides provisions on standardization, conformity assessment, and certification procedures for AI systems. Articles 40 to 49 elaborate on harmonized standards, conformity assessment protocols, EU Declaration and CE marking of

Conformity, and registration requirements to facilitate compliance and interoperability.[138]

- Chapter IV: Transparency Obligations for Providers and Deployers of Certain AI Systems and GPAI Models

Chapter IV emphasizes transparency requirements for providers and users of specific AI systems and Global Partnership on Artificial Intelligence (GPAI) models. Article 50 underscores the transparency obligations in AI development and deployment.[139]

- Chapter V: General Purpose AI Models

Chapter V addresses the classification and regulation of general-purpose AI models, particularly those presenting systemic risks. This contains 3 sections:

- Section 1: Classification Rules
  This part establishes classification rules for general-purpose AI models with systemic risk. Articles 51 to 52 outline the classification process and associated procedures.
- Section 2: Obligations for Providers of General-Purpose AI Models
  This part delineates obligations for providers of general-purpose AI models, emphasizing transparency and accountability. Articles 53 and 54 specify compliance measures and the appointment of authorized representatives.
- Section 3: Obligations for Providers of General Purpose AI Models with Systemic Risk
  This part imposes additional obligations on providers of general-purpose AI models with systemic risk. Articles 55 and 56 emphasize adherence to codes of practice and measures to mitigate systemic risks.[140]

- Chapter VI: Measures in Support of Innovation

This chapter introduces measures to support innovation in AI while ensuring safety and compliance. Articles 57 to 63 elaborate on regulatory sandboxes, informed consent for

[138] EU Artificial Intelligence Act. (n.d.), Chapter III: High-Risk AI System https://artificialintelligenceact.eu/chapter/3/

[139] EU Artificial Intelligence Act. (n.d.)., Chapter IV: Transparency Obligations for Providers and Deployers of Certain AI Systems and GPAI Models, https://artificialintelligenceact.eu/chapter/4/

[140] EU Artificial Intelligence Act. (n.d.)., Chapter V: General Purpose AI Models https://artificialintelligenceact.eu/chapter/5/

testing, and measures to assist small and medium enterprises (SMEs) and startups in navigating regulatory requirements.[141]

➢ Chapter VII: Governance

This chapter establishes governance structures at the union and national levels to effectively oversee AI regulation. This is subdivided into two sections:

- Section 1: Governance at Union Level
  This section provides the provisions for the establishment of the AI Office and the European Artificial Intelligence Board to coordinate regulatory efforts and provide guidance on AI governance. Articles 64 to 69 outlines the board's composition, functions, panel's mandate, mechanisms for member-state engagement and advisory mechanisms.
- Section 2: National Competent Authorities
  This section designates national competent authorities responsible for implementing and enforcing AI regulations at the national level. Article 70 requires that each Member State shall establish or designate at least one notifying authority and at least one market surveillance authority for the purpose of this Regulation as national competent authorities. It further specifies the designation process and the establishment of single points of contact for coordination.[142]

➢ Chapter VIII: EU Database for High-Risk AI Systems

This Chapter establishes a centralized database for high-risk AI systems listed in Annex III. Article 71 outlines the database's purpose and mechanisms for information sharing among stakeholders.[143]

➢ Chapter IX: Post-Market Monitoring, Information Sharing, Market Surveillance

This part focuses on post-market monitoring, incident reporting, and market surveillance mechanisms to ensure ongoing compliance and safety. This chapter is subdivided into 3 sections:

[141] EU Artificial Intelligence Act. (n.d.)., Chapter VI: Measures in Support of Innovation https://artificialintelligenceact.eu/chapter/6/

[142] EU Artificial Intelligence Act. (n.d.)., Chapter VII: Governance https://artificialintelligenceact.eu/chapter/7/

[143] EU Artificial Intelligence Act. (n.d.)., Chapter VIII: EU Database for High-Risk AI Systems https://artificialintelligenceact.eu/chapter/8/

- Section 1: Post-Market Monitoring
  This part mandates post-market monitoring by providers and outlines requirements for monitoring plans for high-risk AI systems. Article 72 emphasizes continuous surveillance to detect and mitigate risks promptly.
- Section 2: Sharing of Information on Serious Incidents
  This part introduces mechanisms for reporting serious incidents involving AI systems. Article 73 emphasizes the importance of transparent reporting to facilitate timely interventions and prevent harm.
- Section 3: Enforcement
  This section outlines enforcement measures to ensure compliance with regulatory requirements. Articles 74 to 84 provide provisions for market surveillance, enforcement procedures, remedies for non-compliance, and procedural rights for economic operators.
- Section 4: Remedies
  This section deals with the remedies available to any natural or legal persons having grounds to consider that there has been an infringement of any of the provisions of the Act. These provisions are attached to Articles 85 to 87 under this section.
- Section 5: Supervision, Investigation, Enforcement and Monitoring in Respect of Provisions of General-Purpose AI Models
  This section contains Articles 88 to 94, which provide for the monitoring actions, procedural rights of operators and different powers of the AI Office with respect to the enforcement of General-Purpose AI Models.[144]

- Chapter X: Codes of Conduct and Guidelines

This Chapter promotes voluntary adherence to codes of conduct to uphold ethical standards and best practices in AI development and deployment. Article 95 and 96 encourages stakeholders to adopt specific requirements for responsible AI use.[145]

- Chapter XI: Delegation of Power and Committee Procedure

[144] EU Artificial Intelligence Act. (n.d.)., Chapter VIII: EU Database for High-Risk AI Systems https://artificialintelligenceact.eu/chapter/8/

[145] EU Artificial Intelligence Act. (n.d.)., Chapter X: Codes of Conduct and Guidelines https://artificialintelligenceact.eu/chapter/10/

This chapter provides procedures for delegating power and committee operations to ensure effective governance of AI regulations. Articles 97 and 98 specify delegation mechanisms and committee procedures for decision-making.[146]

- Chapter XII: Confidentiality and Penalties

This chapter addresses confidentiality provisions and penalties for non-compliance with regulatory requirements. Articles 99 to 101 outline penalties, fines for providers of General-Purpose AI Model and administrative fines for violations.[147]

- Chapter XIII: Final Provisions

This chapter includes final provisions related to amendments, evaluations, and the entry into force of the regulations. Articles 102 to 113 outline amendments to existing regulations, evaluation mechanisms, and the effective date of the regulatory framework.[148]

KEY INSIGHTS FROM THE ACT

The provisions of the AI Act, as briefly explained upon previously, is expected to be a thorough regulatory framework that encompasses a wide array of facets pertaining to AI systems currently understood by humanity. However, within this expansive document, specific provisions stand out as particularly pertinent to the analysis conducted in this research. The major takeaways from the Act that are relevant to the scope of this research are discussed below.

DEFINING AI SYSTEMS

The provisions outlined throughout the Act aim to establish a comprehensive EU-wide legislative framework applicable to all AI systems distributed or utilized within the Union. Drawing upon Article 114 and Article 16 of the Treaty on the Functioning of the European Union (TFEU) and guided by the principles of the New Legislative Framework (NLF), which emphasizes conformity assessments and CE marking for products entering the EU market, the Union seeks to legally define 'AI systems' encompassing various software-based technologies including 'machine learning', 'logic and knowledge-based'

[146] EU Artificial Intelligence Act. (n.d.)., Chapter XI: Delegation of Power and Committee Procedure https://artificialintelligenceact.eu/chapter/11/
[147] EU Artificial Intelligence Act. (n.d.)., Chapter XII: Confidentiality and Penalties https://artificialintelligenceact.eu/chapter/12/
[148] EU Artificial Intelligence Act. (n.d.)., Chapter XIII: Final Provisions https://artificialintelligenceact.eu/chapter/13/

systems, and 'statistical' approaches. This definition may evolve with technological advancements through delegated acts. The now-given definition of artificial intelligence systems in Article 3 (1) of the Act aligns with internationally recognized criteria, following OECD guidelines, which define an AI system as:

> *"a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."*[149]

This wide definition extends across various domains, encompassing nearly every sector. The exceptions lie in specialized areas like military and defence, where stringent regulations apply, along with realms of research, innovation, and casual utilization, where AI finds its limitations. On the contrary, Ebers and colleagues argue that the expansive definition of 'AI systems' could result in legal ambiguity for those involved in their development, operation, and utilization, potentially leading to excessive regulation. They suggest that EU legislators should carve out exemptions for AI systems intended for research and open-source software to mitigate these concerns. Additionally, some critics have raised doubts about the technology neutrality of the definition, noting its focus on 'software' and its potential exclusion of forthcoming AI advancements.

RISK-BASED APPROACH

The Act establishes a risk-based approach where regulatory measures correspond to the level of risk posed. The Act categorises these risks as: "Minimal Risk," "Limited Risk," "High Risk," and "Unacceptable Risk." Systems falling under minimal or no-risk, such as spam filters and AI-driven video games, are not subject to the regulations outlined in the AI Act. For limited risk systems, like chatbots, adherence to transparency measures is mandated, including informing users about the utilization of AI. Additionally, these regulations compel companies, regardless of their origin, to adhere to copyright laws and disclose summaries of their training data. High risk systems, such as those employed in healthcare or education, must provide technical documentation, incorporate human oversight, undergo conformity assessments, among other requirements. Furthermore,

[149] EU Artificial Intelligence Act. (n.d.)., Article 3: Definitions, https://artificialintelligenceact.eu/article/3/

individuals have the right to receive explanations regarding decisions made by these AI systems. Unacceptable risk systems, such as biometric identification systems, are prohibited under the AI Act, except for specific circumstances related to law enforcement. One instance where authorization may be granted for their use is in counterterrorism efforts, albeit with stringent conditions.[150]

HIGH-RISK AND PROHIBITED AI SYSTEMS

AI systems categorized as 'High risk' according to the Act are subjected to additional obligations. These high-risk AI systems fall under specific criteria as outlined in Article 6 of the Act. They include systems used as safety components or products covered by EU laws listed in Annex II, which require third-party conformity assessment under those laws. Additionally, AI systems under certain use cases listed in Annex III are considered high-risk, except under certain conditions. For instance, if the AI system performs a narrow procedural task, enhances the outcome of a previously executed human activity, detects decision-making patterns without replacing human assessment, or undertakes preparatory tasks relevant to Annex III use cases.[151]

Furthermore, AI systems are automatically classified as high-risk if they engage in profiling individuals, which involves automated processing of personal data to evaluate various aspects of an individual's life, such as work performance, economic status, health, preferences, interests, behaviour, location, or movement. Providers of AI systems falling under Annex III, who believe their systems do not pose high risk, are required to document their assessment before introducing them to the market or putting them into operation.

Providers of high-risk AI systems are obligated to adhere to certain requirements outlined in Articles 8 to 27 of the Act. These include establishing a comprehensive risk management system throughout the AI system's lifecycle, ensuring data governance by employing relevant and representative datasets free from errors, and compiling technical documentation to demonstrate compliance with regulatory standards. Moreover, they must design their systems for record-keeping purposes, enabling automatic recording of events to identify risks and substantial modifications. Instructions for downstream deployers must be

[150] EU Artificial Intelligence Act. (n.d.)., High-level summary of the AI Act https://artificialintelligenceact.eu/high-level-summary/

[151] EU Artificial Intelligence Act. (n.d.)., Section 1: Classification of AI Systems as High-Risk https://artificialintelligenceact.eu/section/3-1/

provided to ensure compliance, along with mechanisms for human oversight and measures to achieve accuracy, robustness, and cybersecurity. Additionally, providers are required to establish a quality management system to ensure ongoing compliance with regulatory mandates.

Furthermore, Chapter II, Article 5 of the Act outlines specific types of AI systems categorized as 'Prohibited' under its provisions. Firstly, AI systems that utilize subliminal, manipulative, or deceptive techniques aimed at distorting behaviour and impairing informed decision-making processes, thereby causing significant harm. Secondly, AI systems that exploit vulnerabilities related to age, disability, or socio-economic circumstances to manipulate behaviour, resulting in significant harm. Thirdly, biometric categorization systems that infer sensitive attributes such as race, political opinions, trade union membership, religious or philosophical beliefs, sexual orientation, or sex life, except in cases of lawfully acquired biometric datasets or law enforcement categorization purposes. Additionally, social scoring systems that evaluate or classify individuals or groups based on social behaviour or personal traits, leading to detrimental treatment. Moreover, AI systems that assess the risk of an individual committing criminal offenses solely based on profiling or personality traits, with exceptions for objective, verifiable facts linked to criminal activity. Furthermore, the compilation of facial recognition databases through untargeted scraping of facial images from the internet or CCTV footage. Additionally, the inference of emotions within workplace or educational settings, excluding medical or safety reasons. Finally, the 'real-time' remote biometric identification (RBI) in publicly accessible spaces for law enforcement purposes, with specific exceptions for cases involving missing persons, abduction victims, prevention of substantial threats to life or terrorist attacks, and identification of suspects in serious crimes like murder, rape, armed robbery, narcotics and illegal weapons trafficking, organized crime, and environmental crimes. These provisions within the AI Act aim to establish clear boundaries and guidelines for developing and deploying AI systems, ensuring ethical and responsible practices while minimizing potential risks and harms to individuals and society.[152]

Some AI systems designed for human interaction or content creation may present a potential for impersonation or deception, regardless of their classification as high-risk AI. These systems are obligated to adhere to transparency standards, ensuring that users are

[152] EU Artificial Intelligence Act. (n.d.)., Article 5: Prohibited Artificial Intelligence Practices https://artificialintelligenceact.eu/article/5/

informed when they engage with chatbots. Furthermore, providers of AI systems responsible for generating or altering visual, auditory, or video content (e.g., deep fakes) must disclose their artificial nature, except in rare instances where it serves to prevent criminal activity. Additionally, providers of AI systems generating substantial volumes of synthetic content must employ reliable, interoperable, and robust methods, such as watermarks, to indicate that the output is AI-generated rather than human-produced. Employers deploying AI systems in workplaces must notify employees and their representatives accordingly.

GENERAL-PURPOSE AI MODELS

In the first partial compromise Council text, the Slovenian Presidency of the Council of the EU introduced a new Article specifically addressing General Purpose AI systems. Subsequently, multiple member states have contributed feedback and suggestions on this aspect. As a result, a distinct section, Chapter V, has now been established to govern these General-Purpose AI models.[153] GPAI, in essence, refers to an artificial intelligence model that exhibits broad versatility and competency across various tasks, irrespective of its market deployment method. GPAI models are defined in the Act under Article 3 (44b) which states that a GPAI model means;

> *"an AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable to competently perform a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications. This does not cover AI models that are used before release on the market for research, development and prototyping activities."*[154]

This includes models trained extensively with self-supervised learning on large datasets. These models can seamlessly integrate into different systems and applications. However, it excludes AI models exclusively utilized for research, development, and prototyping purposes prior to market release. A GPAI system, built upon such a versatile AI model, is capable of serving multiple functions, both independently and when integrated into other AI systems. These systems may encompass high-risk AI applications or be

[153] European Union, General Purpose AI and the AI Act: A First Look (May 2022) https://artificialintelligenceact.eu/wp-content/uploads/2022/05/General-Purpose-AI-and-the-AI-Act.pdf
[154] Article 3: Definitions, supra note 136, at 65

incorporated into them. Providers of GPAI systems are encouraged to collaborate with providers of high-risk AI systems to ensure compliance. Providers of GPAI models must adhere to several obligations:

1. Create technical documentation detailing the training and testing processes, along with evaluation outcomes.

2. Furnish information to downstream providers intending to integrate the GPAI model, ensuring they understand its capabilities and limitations for compliance purposes.

3. Establish a policy aligning with the Copyright Directive.

4. Publish a sufficiently detailed summary of the training data utilized for the GPAI model.[155]

In cases of free and open license GPAI models—where parameters, architecture, and usage are publicly accessible—providers are only obligated to meet the latter two requirements unless the model is considered systemic. GPAI models pose systemic risks when the aggregate computational effort used for training surpasses 1025 floating point operations (FLOPs). Providers must promptly inform the Commission if their model meets this criterion, though they can argue that despite meeting the criteria, their model does not present systemic risks. The Commission, or a qualified alert from an independent scientific panel, can determine whether a model possesses high-impact capabilities, rendering it systemic. Providers of GPAI models with systemic risk must fulfil additional obligations:

1. Conduct and document adversarial testing to identify and mitigate systemic risks.

2. Assess and mitigate potential systemic risks and their sources.

3. Report significant incidents and corrective actions promptly to the AI Office and relevant national competent authorities.

4. Ensure robust cybersecurity measures are in place.[156]

All GPAI model providers may demonstrate compliance by voluntarily adhering to a code of practice until European harmonized standards are established. Compliance with

[155] EU Artificial Intelligence Act. (n.d.)., Section 2: Obligations for Providers of General-Purpose AI Models https://artificialintelligenceact.eu/section/5-2/

[156] EU Artificial Intelligence Act. (n.d.)., Section 3: Obligations for Providers of General-Purpose AI Models with Systemic Risk, https://artificialintelligenceact.eu/section/5-3/

such standards will presume conformity. Providers opting out of codes of practice must demonstrate alternative compliance methods approved by the Commission.

The general Codes of practice:

1. Will consider international perspectives.

2. Will cover obligations such as technical documentation specifics for authorities and downstream providers, identification of systemic risks and their sources, and risk management modalities tailored to address challenges within the value chain.

3. AI Office may engage GPAI model providers, national competent authorities, civil society, industry, academia, downstream providers, and independent experts in formulating these codes.[157]

GOVERNANCE AND ENFORCEMENT

Chapter VII of the Act establishes governance structures at the union and national levels to effectively oversee the AI regulation. While AI systems will adhere to the national-level market surveillance system, these regulations concerning GPAI models establish a more centralized oversight and enforcement mechanism. To facilitate this, the AI Office is established as a novel governance entity tasked with specific responsibilities pertaining to GPAI models and closely collaborating with the scientific community to bolster its endeavours. Furthermore, the governance framework provides an enhanced role to the AI Board, broadening its scope of tasks to empower Member States with greater coordination responsibilities. This includes overseeing AI regulatory sandboxes, engaging in consultations with stakeholders, and conducting awareness-raising initiatives. Additionally, the AI Board will furnish opinions to the Commission regarding qualified alerts related to general-purpose AI models, maintaining the composition and operational modalities as per the Council's General Approach.[158]

The Act also introduces two new advisory bodies. A scientific panel comprised of independent experts[159] will furnish technical counsel to the AI Office[160] and market

[157] EU Artificial Intelligence Act. (n.d.)., Article 56: Codes of Practice https://artificialintelligenceact.eu/article/56/

[158] EU Artificial Intelligence Act. (n.d.)., Article 65: Establishment and Structure of the European Artificial Intelligence Board, https://artificialintelligenceact.eu/article/65/

[159] EU Artificial Intelligence Act. (n.d.)., Article 68: Scientific Panel of Independent Experts https://artificialintelligenceact.eu/article/68/

[160] EU Artificial Intelligence Act. (n.d.)., Article 64: AI Office, https://artificialintelligenceact.eu/article/64/

surveillance authorities, playing a pivotal role in enforcing regulations for GPAI models by issuing qualified alerts to the AI Office. Member States will have the opportunity to enlist the support of scientific panel experts to bolster their market surveillance efforts, adhering to the principles set forth in the General Approach. Additionally, an advisory forum will gather stakeholder perspectives for the Commission (including the AI Office) and the AI Board, encompassing a diverse array of stakeholders such as industry representatives, startups, SMEs, civil society, and academia. Lastly, concerning the appointment of multiple competent authorities stipulated in Article 70, the Act grants Member States the flexibility to designate at least one notifying authority and one market surveillance authority as national competent bodies. Moreover, Member States are mandated to designate a single market surveillance authority to serve as a primary point of contact.[161]

The penalties for violating different aspects of the AI Act and the confidentiality aspects have been discussed in Chapter XII of the Act. The practices failing to comply with the regulations regarding prohibited AI practices outlined in Article 5 will result in a penalty of 35 million EUR or 7% of annual turnover.[162] Additionally, Article 101 specifies fines for providers of general-purpose AI models who breach their obligations or fail to comply with enforcement measures, such as providing requested information. The maximum fines for these providers have been aligned with those for providers of high-risk AI systems. It's worth noting that providers of general-purpose AI models will have an extra grace period, with no fines imposed during the first year after the rules come into effect.[163]

[161] EU Artificial Intelligence Act. (n.d.)., Article 70: Designation of National Competent Authorities and Single Point of Contact, https://artificialintelligenceact.eu/article/70

[162] EU Artificial Intelligence Act. (n.d.)., Article 99 (3): Penalties, https://artificialintelligenceact.eu/article/99/

[163] EU Artificial Intelligence Act. (n.d.)., Article 101: Fines for Providers of General-Purpose AI Models https://artificialintelligenceact.eu/article/101/

CHAPTER 5

THE IMPERATIVE FOR GLOBAL AI REGULATORY FRAMEWORK IN THE ADVENT OF EU'S AI ACT

INTRODUCTION

In the preceding chapters, we analysed the rapid evolution of AI and its transformative influence across diverse domains and industries. In the previous chapter, we specifically looked into the provisions of the EU's AI Act, which claims to be the foolproof plan for AI regulation. But AI emerges as a double-edged sword, presenting both remarkable advantages and inherent complexities. This dichotomy underscores the pressing need to address multifaceted concerns surrounding AI, encompassing its identification, utilization, governance, and ethical implications. Among these concerns are potential biases, privacy infringements, and safety hazards, highlighting the imperative for robust regulatory frameworks. Governments worldwide are increasingly cognisant of the imperative to regulate AI to navigate its profound societal impacts effectively. The global nature of AI necessitates cohesive international efforts to establish harmonized laws that promote responsible and accountable AI development and deployment. Such laws not only foster cross-border collaboration but also mitigate conflicts and ensure adherence to ethical standards in AI applications. Crucially, they serve as a conduit for setting universal benchmarks in data protection, privacy safeguards, accountability mechanisms, and transparency protocols, thereby fostering a unified approach to AI compliance. The formulation of international AI laws holds significant promise for advancing global interests, fostering innovation, and averting regulatory fragmentation. Moreover, it provides a vital framework for addressing ethical considerations, safeguarding human rights, protecting vulnerable populations, and upholding core societal values. As such, the global community stands to benefit immensely from concerted efforts aimed at cultivating international cooperation and coherence in AI regulation.

This chapter deals with the urgent necessity for a comprehensive global AI regulatory framework, against the advent of the European Union's landmark AI Act. It scrutinizes the limitations of the AI Act and its potential global ramifications, with particular emphasis on its implications for India and pertinent policy considerations for the nation. Furthermore, it underscores the imperative for AI regulation, elucidating the manifold challenges involved and delineating the roles of various international entities in shaping the overarching regulatory framework for AI.

SHORTCOMINGS OF EU’S AI ACT

The analysis of the various provisions of the AI Act very well shows that it is able to achieve its intended objectives. Adopting a framework grounded in product safety provides a sense of legal assurance, leveraging existing product safety regulations to which providers are already subject in many cases. Expanding this approach to include dangers to fundamental rights tackles various challenges related to AI applications, especially in the public sphere. Notwithstanding these unique features, the Act has faced criticism from a global audience. Examining the criticisms of the Act is outside the scope of this research and will involve more technical details. Nevertheless, it is essential to highlight a significant conflict between the framework's objective of protecting fundamental rights and the use of product safety mechanisms to accomplish this objective.

Product safety regulation often assesses risks related to bad events by considering their probability and severity. However, this approach fails to appropriately consider the diverse dangers posed to basic rights. This encompasses the hazards that arise from elements of fundamental rights that are not clearly quantifiable or from the combined effect of seemingly harmless acts. As a result, the Act's method of safeguarding basic rights by using similar procedures as those used for addressing health and safety hazards brings about a new danger: the possibility of overlooking important types of harm to these rights.[164]

Another important aspect requiring clarity within the Act is to the entities that are required to comply with its terms. More precisely, the Regulation makes a clear differentiation between deployers and providers. The assignment of compliance obligations adheres to a "distributed responsibility" framework, with the objective of preventing excessive burdens on any individual party, at least in theory. A provider is broadly defined as any entity involved in developing an AI system and bringing it to market or utilizing it in a service capacity.[165] The Regulation imposes rigorous obligations on providers, especially

[164] Paolucci, F, *Shortcomings of the AI Act: Evaluating the New Standards to Ensure the Effective Protection of Fundamental Rights,* Verfassungsblog (March 14, 2024), https://verfassungsblog.de/shortcomings-of-the-ai-act/#:~:text=The%20AI%20Act%20distinguishes%20between,uses%20are%20considered%20high%2Drisk.

[165] EU Artificial Intelligence Act. (n.d.)., Article 3 (2): Definitions, https://artificialintelligenceact.eu/article/3/

for high-risk AI systems, emphasizing adherence to European legal standards and principles of accountability. On the other hand, a deployer is an entity that uses an AI system inside its control, but does not include non-professional personal activities.[166] Deployers are often required to guarantee compliance with CE standards. Furthermore, deployers take on increased accountability when they make changes to the fundamental model of a generative artificial intelligence system. As it depends on how one interprets the legal requirement of "substantial modification" of the system, as stated in Article 3, determining who qualifies as a provider or deployer is legally difficult.

The law seeks to hold generative AI implementers accountable, but only if they alter core models. Nevertheless, the Regulation lacks explicit instructions on the specific criteria for revisions that would satisfy this criterion. Therefore, it is uncertain under what circumstances a provider would be exempt from liability for interventions on the AI model that are exclusively performed by the deployer. Thus, the practical application of rules governing AI systems becomes a major concern. Although the regulations for high-risk AI are extensive, they are often formulated in abstract terms, necessitating substantial interpretation efforts by AI system providers. This places providers in the position of determining how legal requirements translate into software requirements, presenting technical challenges, particularly for translating vague legal principles into computer code. Due to the complexity and scope of many AI systems, correcting errors in representation or adjusting to legal changes can be a time-consuming operation. This might result in the providers of these systems establishing arbitrary or inaccurate interpretations of the law. Although the Act include methods to offer direction and minimise subjective interpretation by providers, such as mandating external certification and relying on standardised criteria, these mechanisms encounter difficulties. Private entities typically produce technical standards and certification schemes through closed deliberations that are not open to the general public. As a result, there are ongoing concerns about the credibility of these external players in establishing rules that try to safeguard basic rights, due to their intrinsic separation from wider community viewpoints.

The Act necessitates careful deliberation about the responsibilities of providers and deployers, taking into account the measures currently in place under current European and Regional laws. This is especially important in relation to data protection laws. The Act

[166] EU Artificial Intelligence Act. (n.d.)., Article 3 (4): Definitions, https://artificialintelligenceact.eu/article/3/

incorporates a "fundamental rights impact assessment" as a means of ensuring compliance. This evaluation is designed to identify and resolve specific dangers to persons' rights. Deployers of high-risk systems specified in Article 26 of the Act are required to comply with this obligation.[167] In addition, if a deployer is classified as a "data controller," with the responsibility of defining the purpose and methods of data processing according to data protection law, they are also required to carry out a Data Protection Impact Assessment (DPIA) as stated in Article 27 of the Act.[168] A data processor, or provider, acts as an intermediary between the controller and the data. According to the GDPR, service providers are classified based on the level of control they have over an AI system. To impose additional duties under data protection laws, data protection authorities may designate a provider as a data controller or joint controller with the deploying firm if the provider has substantial influence, including over basic models. However, potential challenges in bringing the Act into accordance with current EU legislation are highlighted by the lack of clarity regarding the level of control a provider has to be designated as a data processor. According to Articles 15–22 of the GDPR, this clarification is necessary to provide rights for individuals, clarify responsibilities among parties, and provide legal certainty.[169]

There are now substantial legal and technical challenges to administering biometric recognition technologies in compliance with Articles 5, 6, and 26 of the Act. This is yet another matter that needs clarity. The Act differentiates between two types of biometric data applications: those that compare faces instantly (known as "real-time" applications) and those that perform recognition later on (known as "ex-post" applications). In general, it is not recommended to utilise it in real-time, and using it after the fact is considered risky. With the exclusions specified in Article 5 of the Act, it is specifically illegal for law enforcement to use real-time biometric identification in publicly accessible locations. According to paragraph 2 of Article 6, ex-post biometric identification methods are considered high-risk AI systems.[170] Systems for emotional recognition and biometric classification fall under this umbrella. It is critical to understand this regulation in conjunction with the above discussed Article 26 and Annex III. Importantly, this use is

[167] EU Artificial Intelligence Act. (n.d.)., Article 26: Obligations of Deployers of High-Risk AI Systems https://artificialintelligenceact.eu/article/26/

[168] EU Artificial Intelligence Act. (n.d.)., Article 27: Fundamental Rights Impact Assessment for High-Risk AI Systems, https://artificialintelligenceact.eu/article/27/

[169] General Data Protection Regulation (GDPR), Chapter 3 – Rights of the data subject, (October 5, 2018), https://gdpr-info.eu/chapter-3/

[170] EU Artificial Intelligence Act. (n.d.)., Article 6 (2): Classification Rules for High-Risk AI Systems https://artificialintelligenceact.eu/article/6/

limited to certain instances and requires approval from an administrative or judicial body. This means that broad or careless use is not allowed unless it is explicitly linked to a criminal threat, current legal processes, or the hunt for a missing individual.

Having said that, this body of law does bring up a few questions. In particular, the Joint Opinion of the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB) stresses, from a basic rights standpoint, how irrelevant it is to differentiate between ex-post and real-time biometric recognition. There is a technical distinction with comparable implications for citizen surveillance that determines how intrusive processing is, rather than whether identification or recognition occurs first. Whether employed in real-time or after the fact, the fundamental biometric system, which is trained using a dataset, does not change.[171] The fact that Member States have a lot of leeway to decide how to use biometric systems, especially with regard to the permission procedure described in Article 5, paragraph 2, is another major worry with biometric recognition. There are certain grey areas in the Regulation, even if it does lay out the parameters for system use. The decision of whether biometric recognition should be authorised by a judicial or independent administrative authority is left to the Member States.

In our opinion, Member States should support judicial authority since it might be the most efficient manner. Following the precedent set by the European Court of Justice in the Corbiau case,[172] it is essential to guarantee judicial independence and transparency when making decisions that substantially affect individual rights. An essential component of the rule of law, the Court emphasised the need for independence in deciding whether an entity is capable of being a court or tribunal. Also, there needs to be a lot of reason; the European Court of Human Rights pointed out flaws in the permission process for facial recognition in public places in Glukhin v. Russia.[173] This requirement can be met via judicial independence. Accordingly, in order to protect rights and procedural justice, Member States should make sure that such authorizations are handled solely by judicial authorities, while yet maintaining procedural independence.

[171] European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB), Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), (June 18, 2021), www.edpb.europa.eu. https://www.edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

[172] Pierre Corbiau v Administration des Contributions, European Court reports 1993, Page I-01277. The European court of Justice in this case held that the concept of a court of tribunal, within the meaning of Article 177 of the Treaty, is a concept of Community law and by its very nature can embrace only authorities acting as a third party in relation to the authority which adopted the decision under appeal.

[173] Glukhin v. Russia - 11519/20 4 July 2023 [Section III], European Court of Human Rights

Emotion recognition systems are currently considered a high-risk use of AI according to the Act,[174] and judicial control of the authorization process is an important factor in determining their use. Although emotion recognition is not allowed in educational or workplace settings according to the Regulation, it can be used in other contexts as long as it meets the requirements for systems with high risk. Nevertheless, there is significant ambiguity in Article 52, which deals with transparency duties; specifically, it does not state that individuals subjected to biometric or emotional analysis must be notified in cases when AI systems identify, prevent, or investigate criminal activity.

The use of AI in migration scenarios raises similar problems, as individuals whose biometric data is collected are in a particularly vulnerable position. When it comes to border management and control, asylum seekers, visa applicants, and individuals entering or having entered a Member State's territory, polygraphs and systems evaluating security, irregular migration, or health risks are considered high-risk systems.[175] There are ramifications for the authorization of biometric and emotion systems in immigration, asylum, border control, and law enforcement due to the wide range of possible uses, some of which appear to be just as dangerous as those that are forbidden.

Concerns over legal certainty and access to effective remedies arise from Article 59, which allows face recognition in certain situations without consent from courts or other authorities. This could result in inappropriate uses, which is particularly problematic in delicate areas such as migration, where invasive practices are already common. Biometric recognition could be used extensively in situations of irregular migration, going beyond the criminal offences stated in Annex II of the Act, to establish identity upon entry, which is sometimes problematic due to a lack of documents. Particularly in Articles 27 and 70, the Act guarantees procedural rights before the Market Surveillance Authority and ushers in the Fundamental Rights Impact Assessment framework for high-risk systems.[176] However, there are also concerns that people have, such as the possibility of inefficiencies in protecting basic rights and discrepancies in biometric surveillance protocols.

In addition, the hazards linked to susceptible data gathering, along with the inherent power imbalance between individuals and public agencies, highlight the necessity of judicial monitoring. The judiciary's responsibility as a protector of rights is crucial in the field of AI

[174] EU Artificial Intelligence Act. (n.d.)., Annex III para.1 (ab): High-Risk AI Systems https://artificialintelligenceact.eu/annex/3/
[175] EU Artificial Intelligence Act. (n.d.). , Annex III para. 7: High-Risk AI Systems https://artificialintelligenceact.eu/annex/3/
[176] Article 27, supra note 138 at 67

governance, especially when it comes to approving and monitoring the actual implementation of AI. However, if proven, these and other criticisms might weaken the product safety framework of the Act, making it less effective at protecting basic rights. Traditional risk assessment models may fail to take into account intangible concerns, which could lead to the amplification of the power of shadowy private entities to dictate basic human rights and undermine democratic rule and the rule of law. Therefore, the Act, which was supposed to reduce dangers associated with AI in the EU, could end up undermining the principles it claims to support, making its stated goals impossible to achieve.

BRUSSELS EFFECT

As we have seen above and in the previous chapters, the AI Act is about to provide a framework including self-certification processes and government supervision for certain high-risk AI system categories. It also tries to prohibit some "unacceptable" characteristics of AI systems and requires transparency measures for AI systems interacting with people. These AI Act provisions have extraterritorial effects, which means they can impact the creation and use of AI systems anywhere in the globe and may spark similar legislative efforts elsewhere. Multinational companies are strongly encouraged to follow these rules throughout their worldwide operations by the EU, which has set strict criteria within its vast internal market. This phenomenon—called the Brussels Effect—depends on the EU's position as a regulatory heavyweight. Companies that adopt a single set of standards throughout their operations not only reduce administrative costs but also streamline procedures. As such, this commitment promotes the slow Europeanization of international trade, reflecting European goals in fields such as intellectual property, climate change, data privacy, cybersecurity, product safety, financial services, and environmental preservation.[177]

The phrase "Brussels effect" was introduced in 2012 by Professor Anu Bradford from Columbia Law School, inspired by the concept of the "California effect" within the United States. This phenomenon describes how entities, particularly corporations, tend to adhere to EU regulations even outside of the EU due to various factors. Instances of the Brussels Effect encompass the influence exerted by EU Competition Laws, Antitrust laws, and regulations pertaining to consumer health and safety within the chemical sector, such as those outlined in the 2003 Restriction of Hazardous Substances Directive. This phenomenon is notably

[177] Charlotte Siegmann and Markus Anderljung, *The Brussels Effect and Artificial Intelligence: How EU Regulation Will Impact the Global AI Market*, Centre for the Governance of AI, (August 16, 2022)**,** https://www.governance.ai/research-paper/brussels-effect-ai

evident in the widespread adoption of the GDPR as a benchmark for global data protection standards. Likewise, the potential for the AI Act to establish a universal standard, thereby compelling multinational corporations to adhere to EU market requirements, underscores the Brussels Effect. The Brussels Effect operates discreetly, leveraging market dynamics rather than overt geopolitical or economic coercion. It embodies a contemporary manifestation of soft power, where the EU's influence emanates from the allure and efficacy of its regulatory frameworks. Beyond mere influence outside the EU's confines, the Brussels Effect carries significant implications, notably the EU's capacity to unilaterally establish standards that evolve into global benchmarks, not through coercion, but through the appeal of its vast consumer base numbering 450 million.[178]

DE FACTO BRUSSELS EFFECT

A de facto Brussels Effect materializes when companies opt to adhere to EU regulations in regions beyond the EU's jurisdiction without any obligatory mandate from those regions. Whenever the EU enforces new regulations, multinational corporations encounter a dual dilemma. Firstly, they need to assess whether remaining in the EU market remains viable. The introduction of new regulations might potentially shrink market size and profit margins to the extent that operating within the EU market becomes unprofitable. Secondly, assuming companies choose to continue operating within the EU market, they must then decide whether to extend compliance with the new regulations globally or to offer two distinct products: one compliant with EU standards and another non-compliant for regions outside the EU. A de facto Brussels Effect occurs if companies opt to stay in the EU market and market EU-compliant products worldwide. Anu Bradford's works, including the 2020 book "The Brussels Effect" and a 2012 paper of the same title, outline five pivotal factors contributing to the de facto Brussels Effect:

1. Favourable Market Properties: The sheer size of the EU market significantly influences companies' decisions, with larger markets correlating with higher chances of companies maintaining their presence despite regulatory changes. Moreover, a greater relative size of the EU market increases the likelihood of companies opting to sell EU-compliant products globally. Additionally, markets characterized by

[178] Bradford, A, *The Brussels Effect*, Oxford University Press, USA (January 1, 2020). http://books.google.ie/books?id=mZXHDwAAQBAJ&printsec=frontcover&dq=The+Brussels+Effect:+How+the+European+Union+Rules+the+World&hl=&cd=1&source=gbs_api

oligopolistic structures dominated by multinational corporations are more prone to experiencing de facto regulatory diffusion.

2. Stringency: For a de facto Brussels Effect to occur, EU regulations must surpass the standards of regulations in other jurisdictions on certain dimensions.
3. Regulatory Capacity: The ability of a jurisdiction to craft and enforce well-designed legislation plays a crucial role. Early and effective implementation of regulations, coupled with the capacity to enforce compliance, reduces regulatory costs and enhances the likelihood of both corporate compliance and consumer acceptance of EU-compliant products.
4. Inelasticity within and outside the EU: Both demand and supply, both within and outside the EU, need to exhibit relative inelasticity to prevent market shrinkage in response to regulatory changes. Lower elasticity within the EU increases the probability of companies maintaining their presence, while lower elasticity outside the EU increases the likelihood of non-differentiation.
5. Costs of Differentiation: Higher costs associated with differentiation, i.e., maintaining separate EU-compliant and non-EU-compliant product lines, increase the likelihood of a de facto effect. The expenses incurred in differentiation, such as higher fixed and variable regulatory costs and duplication costs, contribute to this likelihood.[179]

High-risk systems employed by multinational corporations are particularly susceptible to experiencing a de facto effect. Such systems include those governed by existing EU product safety regulations, such as machinery and medical technology. Additionally, systems utilized for worker management, remote biometric identification, legal tech, and foundation models may also be affected, especially if compliance with EU regulations becomes synonymous with product trustworthiness. Certain requirements of high-risk systems, such as those related to risk management, record-keeping, transparency, accuracy, robustness, and cybersecurity, are more likely to trigger a de facto effect.[180]

DE JURE BRUSSELS EFFECT

The De Jure Brussels Effect comes into play when foreign jurisdictions adopt rules influenced by EU regulations. This can occur through four main channels:

[179] Ibid

[180] Charlotte Siegmann, supra note 177, at 84

1. Blueprint Adoption Channel: Foreign jurisdictions voluntarily adopt EU regulations, either through imitation or learning from the positive outcomes of EU regulations. The EU's regulatory expertise and capacity often result in well-crafted regulations, prompting other jurisdictions to follow suit.
2. Multilateralism Channel: The EU advocates for its regulations in multilateral and bilateral negotiations, influencing international standards organizations like the ISO.
3. De Facto Channel: Multinational corporations, influenced by the de facto Brussels Effect, may lobby non-EU legislators to adopt EU-equivalent standards to avoid market disadvantages. The cost of adopting such standards is lower for jurisdictions where some companies are already compliant.
4. Conditionality Channel: EU trade requirements, extraterritoriality, and economic pressure encourage other countries to adopt regulations equivalent to those of the EU.

The Blueprint Adoption Channel is particularly relevant to AI regulation due to the EU's early adoption advantage and active promotion of AI regulations over recent years. This channel is likely to impact smaller jurisdictions more significantly, especially those without major domestic AI companies. However, the likelihood of a de jure Brussels Effect reaching the US federal level seems lower historically. Yet, regulatory diffusion to individual US states, such as California, which has already adopted GDPR-like data protection laws, could influence future federal regulations. While past instances of de jure Brussels Effects have had limited real-world effects, such as the Product Liability Directive, there is potential for significant impact in specific contexts.[181]

POTENTIAL BRUSSELS EFFECT OF AI ACT

The data protection framework within the EU has demonstrated a robust Brussels Effect in both de jure and de facto terms. This phenomenon is partially facilitated by the global dissemination of the EU-endorsed notion of data privacy as a fundamental human right, a distinctive aspect of European data protection legislation. Notably, countries outside the EU have adopted more stringent data protection provisions, exceeding the requirements for trade with the EU. A study conducted in 2012 revealed that 28 out of 33 analysed data privacy laws incorporated restrictions on exporting data across borders. This underscores

[181] Ibid

the pervasive influence of European data protection regulations beyond its borders. Somewhat similarly, the EU's AI will generate a de facto Brussels Effect.

To ensure that the AI Act generates a Brussels Effect, the significance of market size cannot be overstated. In the currently available data, the EU presents a sizable market for AI systems due to its expansive single market and affluent population. This makes it an attractive destination for providers of AI-based consumer goods. Moreover, major online platforms are unlikely to disregard the access to millions of users located in EU Member States. Additionally, the EU provides substantial opportunities for AI systems marketed for both business and public sector applications. Given that compliance with the AI Act is mandatory for selling AI systems in the EU single market, the risk of exclusion from this market is a significant concern for global AI providers. Furthermore, the AI Act demonstrates the necessary regulatory capacity for a Brussels Effect. As AI is a rapidly evolving technology with limited regulatory precedent, the EU has taken proactive steps to address this challenge. Initially, the EU prioritized the development of expertise in AI, integrating discussions on AI technologies into the reform of data protection laws in the mid-2010s. This included the formation of a high-level expert group comprising individuals from academia, industry, and relevant national and EU bodies. Furthermore, the EU leverages its existing product safety framework, which draws on decades of experience in interpretation and enforcement. This approach minimizes the need to establish entirely new regulatory institutions and practices. Consequently, few jurisdictions possess the technical and institutional capabilities comparable to those available within the EU for regulating AI.[182]

The effectiveness of the AI Act in having a Brussels Effect hinges on its level of rigour. If EU standards surpass those of other regions, adhering to EU regulations typically suffices elsewhere. However, the AI Act faces uncertainties in this regard. It primarily focuses on disclosure obligations for non-prohibited or non-high-risk systems, as outlined in Article 52. Yet, some jurisdictions propose stricter regulations for specific applications, like online recommender systems, or introduce additional measures for non-high-risk AI, often extending beyond the AI Act's technical requirements. Consequently, merely complying with the AI Act might not ensure alignment with all relevant laws across jurisdictions, especially considering its limited scope for such systems. Conversely, the AI

[182] Almada, M., & Radu, A, *The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy*, SSRN Electronic Journal, (2023), https://doi.org/10.2139/ssrn.4592006

Act adopts stringent measures for both high-risk and general-purpose AI systems with systemic risks. Nevertheless, certain public interest concerns associated with AI, particularly those related to fundamental rights, fall outside the purview of product safety frameworks addressed in the Act. Any foreign legislation addressing these unaddressed issues will impose requirements surpassing EU standards. As of March 2024, several domains illustrate where the AI Act exceeds the practices of other jurisdictions: the enactment of new regulations for general-purpose AI systems with systemic risks, the prohibition of certain AI system categories under Article 5, and the regulation of issues already covered by the product safety framework for high-risk AI systems. Consequently, the Brussels Effect is more probable in these aspects of the AI Act.[183]

Another prerequisite for the Brussels Effect to take place involves the regulatory target being inflexible, meaning it's a product or producer that must adhere to a set regulatory framework regardless of its specific characteristics. In the context of the AI Act, there are two forms of flexibility to consider. The first pertains to the Act's scope: if AI providers could easily offer their systems from outside the EU, they would lack the motivation to comply with a stricter regulatory regime. However, the AI Act addresses this by extending its provisions territorially and applying them to any AI system with outputs within the EU, regardless of the provider or user location. While providers technically have the option to leave or enter the EU market, the lucrative size of the market makes it unlikely for major providers to opt-out. Moreover, once providers choose to participate in the EU single market, they have limited leeway to circumvent the Act's scope. The second form of flexibility within the AI Act pertains to the categorization of AI systems under its regulatory frameworks. Providers can avoid regulations applicable to high-risk AI systems by asserting that their systems do not pose significant risks to the values protected by the Act. This exemption does not mandate external assessment or authority ratification but necessitates adherence to guidelines outlined in Article 6 (2a) of the AI Act and any subsequent criteria set by the Commission. However, the Act's definition of general-purpose AI systems features narrow exclusions from its scope, and the determination of systemic risk is predominantly dictated by external evaluation, either through Commission decisions or predefined thresholds.

[183] Musch, S., Borrelli, M., & Kerrigan, C, *The EU AI Act As Global Artificial Intelligence Regulation*, SSRN Electronic Journal (2023), https://doi.org/10.2139/ssrn.4549261

Consequently, while the classification of a system as high-risk under the AI Act is somewhat flexible, rules for general-purpose AI systems are comparatively rigid.[184]

Additionally, the Brussels Effect requires the regulated object to be non-divisible. If providers can develop separate AI systems for the EU market, they can bypass compliance with EU standards elsewhere. This non-divisibility is absent from the regulation of prohibited AI systems, allowing providers to continue marketing these systems in jurisdictions permitting them. Furthermore, certain lawful applications, like AI systems tailored for the public sector, can be segmented due to their highly differentiated nature. Consequently, markets accommodating such segmentation are less likely to experience a significant Brussels Effect. Nevertheless, contemporary approaches to AI discourage divisibility in other applications. Many advancements in AI technologies, particularly those involving general-purpose AI models, rely on machine learning systems demanding substantial data and computing resources for training and operation. Consequently, only a handful of economic actors possess the necessary resources to develop such systems, leading most AI providers to construct their systems compositionally, often starting from components or pre-trained models offered by large-scale providers, who essentially serve as digital infrastructure suppliers. This compositional approach to AI technologies reinforces the AI Act's ability to prevent divisibility. As AI technologies rely on centralized infrastructures, including general-purpose AI systems, smaller providers find it challenging to develop EU-specific versions of their products. Even major providers might find the costs of maintaining EU-specific versions of their infrastructure prohibitive. Thus, market segmentation becomes financially unviable because developing EU-specific products is costlier than globally complying with EU legal requirements. Similarly, reliance on components and general-purpose AI tools fosters non-divisibility within the EU market, as low-risk AI systems constructed using such tools inherently comply with some of the tools' technical standards.[185]

Based on the above analysis, it can be concluded that there will be a limited but serious Brussels Effect for the AI Act. Market dynamics alone cannot fully extend the EU's restrictions on certain AI uses or its regulations concerning AI systems outside the more tightly controlled categories. Even within these categories, the adoption of EU standards

[184] Engler, A, *The EU AI Act will have global impact, but a limited Brussels Effect*, Brookings (June 8, 2022), https://www.brookings.edu/articles/the-eu-ai-act-will-have-global-impact-but-a-limited-brussels-effect/

[185] Almada, M., supra note 182, at 88

relies on factors like product differentiation and the adequacy of the product safety framework in addressing pertinent regulatory issues. However, the intricate technical nature of AI governance complicates the anticipation of situations where alternative standards might surpass the EU approach in stringency. Consequently, the EU's standard for high-risk AI is likely to influence the global governance of such applications.

RISK OF BRUSSELS SIDE EFFECT

The potential consequence of the AI Act resembling a Brussels Effect is a notable concern. It may inadvertently lead to a decrease in safeguarding values beyond product safety measures. While the global adoption of AI safety standards rooted in the AI Act may seem promising, it could inadequately protect fundamental rights, democracy, and the rule of law. In fact, adherence to these standards might introduce new risks by enforcing norms that narrowly interpret these values. The AI Act's deficiencies could result in a global erosion of values integral to the EU legal framework if not rectified during the legislative process. We argue that the mechanism facilitating the global dissemination of standards could weaken the protection of fundamental rights and democratic principles. This effect may arise through the strict technical requirements outlined in the AI Act, leading stakeholders to believe that compliance ensures the safeguarding of values. However, values not explicitly covered by the Act may be overlooked in software design, posing risks that may only surface after causing harm.

Furthermore, while the Brussels Effect in its de jure form may present challenges, its de facto manifestation is more concerning. Unlike the EU, other jurisdictions possess the flexibility to adopt diverse regulatory approaches. Nevertheless, the technical complexity of AI regulation may lead many to emulate the AI Act's approach, despite potential shortcomings. Considering the potential global ramifications, it becomes crucial to contemplate external consequences during the AI Act's legislative process. While some may argue that the EU's responsibility ends at its borders, such a stance contradicts its constitutional obligation to uphold European values globally. The Brussels Side Effect, as termed in this discussion, is a result of the AI Act's alignment with a product safety framework, which fails to adequately address fundamental values. Despite this, it is poised to become a global standard, potentially derailing the EU's ambition to promote its approach to AI regulation worldwide.

IMPACT OF THE AI ACT ON INDIA

Although India has already initiated efforts towards the AI for All initiative,[186] it also collaborated in chairing a meeting with the EU on trade and technology in November 2023. This meeting aimed to enhance the strategic partnership between India and the EU, particularly in areas like trustworthy AI. Consequently, Indian policymakers may consider EU laws as a guiding framework while implementing their own AI For All campaign. This campaign seeks to make AI more accessible to people from diverse backgrounds and educate citizens about its benefits and drawbacks. The recent statement from the Indian Minister of State for IT reaffirmed the government's commitment to leveraging AI positively rather than demonizing it. Additionally, it indicated the government's intention to develop a regulatory model for AI to establish a common standard. The minister's mention of the necessity for an International Alliance on AI underscores the importance of moving beyond theoretical principles to achieve regulatory consistency.[187]

In addition to the numerous regulatory obligations faced by Indian companies catering to clients in the EU, there is an additional consideration regarding how current AI models align with the criteria outlined in the EU Act. While the Act presents opportunities for innovation, it also introduces compliance costs for Indian IT sectors, particularly medium-sized ones. Therefore, it is premature to gauge the direct effects of the EU Act on Indian policies and stakeholders. The diverse secondary implications need consideration and include:

1. Influence of Global Standards: Given the EU's historical role as a regulatory pioneer, businesses worldwide aim to adhere to EU regulations to access its vast market of over 500 million consumers. India may explore aligning some of its AI policies with EU standards to ensure seamless trade and collaboration.
2. Opportunities for Collaboration: India could leverage this alignment to advance its Make in India and Make for World initiatives. Through joint ventures, research endeavours, and standard harmonization, both regions could enhance R&D and promote responsible AI development and deployment.

[186] Niti Ayog, National Strategy for AI #AIFORALL, (2018, June), https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf

[187] Times of India, *India AI Mission: IT Minister on How Government Will Develop Homegrown AI Models*, Timesofindia.Indiatimes.Com. https://timesofindia.indiatimes.com/technology/tech-news/indiaai-mission-it-minister-on-how-government-will-develop-homegrown-ai-models/articleshow/108402685.cms

3. Facilitating Cross-border Data Flows: Collaboration may facilitate the exchange of data and joint efforts in AI research and development.
4. Policy Adaptation: Indian policymakers could glean insights from the implementation of EU regulations, understanding their efficacy and the challenges faced by EU member states, and adapt such experiences to suit the Indian context.

In conclusion, while the EU's AI Act represents a significant step towards regulating AI systems and safeguarding fundamental rights within its jurisdiction, it also faces notable shortcomings and challenges. The Act's reliance on product safety mechanisms to protect fundamental rights introduces a new risk of neglecting significant forms of harm to these rights, particularly those not easily quantifiable in terms of likelihood and severity. Moreover, the ambiguity surrounding the distinction between providers and deployers and the lack of clarity on the threshold for substantial modification pose legal challenges and may lead to uncertainty in liability attribution. The potential Brussels Effect of the AI Act could inadvertently prioritize narrow technical requirements over broader values, risking a global erosion of fundamental rights and democratic principles. These challenges are more faced by the EU’s major trading partners like India. Therefore, while Indian policymakers may consider the EU's regulatory framework as a guiding model, careful consideration of the Act's implications and adaptation to the Indian context are essential to ensure the positive impact of AI regulation on stakeholders in India and beyond. But if every country is going to make its own frameworks to regulate AI without proper international cooperation, then it would create barriers to international trade as such.

THE NEED FOR AN INTERNATIONAL AI REGULATION

As AI systems become increasingly integrated into various aspects of our lives, from healthcare to finance to transportation, the need for comprehensive regulation becomes paramount. The necessity for AI regulation originates from the principle that regulation should have a clear purpose. Thus, regulation should only be implemented if it can effectively bring advantages to both the AI sector and society. Recent advancements in AI, like the EU AI Act, have prompted numerous ethical and legal concerns. Additionally, even private sector entities typically averse to government involvement are acknowledging the risks associated with AI. These factors primarily underscore the need for regulation. Regulation, in this sense, can provide the sector with legal certainty and stability, and even offer incentives and subsidies, allowing it to develop more than it would without intervention.[188] The major reasons for the need to regulate AI are as follows:

- Ambiguity in AI Definition

One of the fundamental challenges in regulating AI lies in the lack of a universally accepted definition of the term "artificial intelligence." Any regulatory framework must precisely delineate what falls under its purview, yet the concept of intelligence itself is inherently complex and multifaceted. Since humans are the primary reference point for intelligence, defining AI becomes entangled with the ambiguity surrounding human cognition.[189] As a result, there is no consensus on a definitive definition of AI, making it challenging to regulate effectively.

- Bias, Privacy, and Ethical Decision-Making

AI systems, if not properly regulated, have the potential to perpetuate and amplify human biases, leading to unfair outcomes in decision-making processes. Whether it's determining loan approvals, contract negotiations, or personalized advertising, AI algorithms can inadvertently discriminate against certain groups or individuals. Moreover, the vast troves of personal data collected by AI systems raise serious concerns about privacy infringement. Without appropriate regulations in place, there is a risk of AI technologies encroaching upon individuals' private lives and exploiting sensitive information for commercial gain. In P.M. et al. v OpenAI LP et al. filed in the Northern District of California the court ruled that the unauthorized gathering, retention, monitoring, and distribution of private information via web scraping without consent constitutes a massive misuse of personal data.[190]

- Economic Implications and Fair Competition

While AI promises increased efficiency and productivity, its widespread adoption raises legitimate concerns about job displacement and economic inequality. As AI automation continues to advance, there is a looming threat of job loss across various sectors, disproportionately impacting vulnerable populations. Additionally, the dominance of large

[188] SpotDraft, *Global AI Regulation: A Comprehensive Guide*, Spotdraft Blog, https://www.spotdraft.com/blog/global-ai-regulation#:~:text=The%20misuse%20of%20AI%20to,it's%20about%20guiding%20it%20responsibly.

[189] Matthew U. Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, 29 Harv. J. L. & Tech. 353 (2016)

[190] P.M. et al. v. OpenAI LP et al, No. 3:23-cv-03199 (N.D. Cal. Jun 28, 2023)

tech companies in the AI market could stifle competition and innovation, creating barriers to entry for smaller businesses. To ensure equitable access and promote fair competition, regulatory measures must be implemented to address these economic challenges.

- Safety, Security, and Autonomy

The autonomous nature of AI systems introduces significant safety and security risks that necessitate regulatory oversight. Whether it's self-driving cars making split-second decisions on the road or autonomous drones navigating complex environments, the potential for accidents and unintended consequences is a pressing concern.[191] Moreover, the opacity of AI decision-making processes poses challenges for accountability and foreseeability. As AI systems become increasingly autonomous and adaptive, there is a risk of losing human control over their actions, leading to unpredictable outcomes and potential harm to society.

- Cyber Threats and Misuse

While AI can enhance cybersecurity measures, it also presents new vulnerabilities and threats in the digital realm. From malicious actors exploiting AI-powered vulnerabilities to the proliferation of deep fake content, the misuse of AI poses significant risks to digital security and societal trust. Regulatory frameworks must address these emerging threats by establishing guidelines for AI development, deployment, and usage to mitigate potential harms and safeguard against malicious activities.[192]

- Liability and Accountability

The evolving nature of AI systems complicates traditional notions of liability and accountability, raising questions about who bears responsibility for AI-related outcomes. With AI's discreet, diffused, and opaque development processes, attributing liability becomes increasingly challenging. Furthermore, the democratization of AI development through open-source platforms enables widespread participation, making it difficult to identify individuals or entities accountable for AI-related incidents. Regulatory efforts must navigate these complexities to ensure accountability while fostering innovation and collaboration in the AI ecosystem.

[191] Lennart S. Lutz, *Automated Vehicles in the EU: A Look at Regulations and Amendments*, GENRE, 12, (March 10, 2018), http://www.genre.com

[192] National Cyber Security Centre, *The Impact of AI on Cyber Threat* (June 14, 2023) https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat#:~:text=AI%20has%20the%20potential%20to,AI%20model%20for%20this%20purpose.

CHALLENGES IN INTERNATIONAL AI REGULATION

The task of regulating AI internationally presents a sophisticated challenge due to many reasons like the diversity inherent in the technology itself. Furthermore, each country brings its unique perspective to the fore, with some offering innovative solutions while others exercise cautious deliberation. This created many hurdles in building a common regulatory framework.

One of the foremost hurdles in AI regulation lies in striking a delicate balance between promoting innovation and ensuring responsible deployment. This equilibrium is paramount as technological advancement should be encouraged globally without compromising the diverse societal values and ethical principles. For instance, the United States, renowned for its Silicon Valley and pioneering tech conglomerates, has embraced a laissez-faire approach, allowing market forces to steer AI development. Despite this, the US remains cognizant of the imperative for responsible AI innovation, juxtaposing technological progress with ethical considerations and societal implications. This duality underscores the necessity of fostering innovation while upholding ethical standards.

The tension between international collaboration and national interests further complicates the landscape of Global AI regulation. While AI transcends geographical boundaries, countries assert their sovereign interests, creating a dynamic interplay between global cooperation and domestic agendas. A pertinent illustration is the above-explained EU's AI Act itself, which underscores Europe's commitment to AI advancement while staunchly safeguarding individual privacy and ethical norms. This legislative initiative sets a high standard for global AI players, emphasizing compliance with the EU's rigorous ethical and privacy criteria. Consequently, varying national priorities and concerns impede consensus on a unified global regulatory framework, accentuating the challenge of reconciling divergent interests.

Moreover, the rapid pace of AI evolution poses a formidable obstacle to the formulation of effective regulatory measures. As AI technology advances exponentially, legal frameworks lag behind, struggling to keep pace with the dynamic landscape. This discordance parallels the incongruity of attempting to operate a Radio with contemporary smartphone technology. In response, countries endeavour to imbue their legal frameworks with agility and adaptability commensurate with the technological landscape they seek to govern. Japan's pragmatic approach to AI regulation exemplifies this adaptability, prioritizing the safety and societal benefits of AI over rigid regulatory constraints. By maintaining a flexible stance, Japan swiftly adjusts to technological advancements, thereby aligning its regulatory framework with the rapid cadence of AI innovation.[193]

Despite these formidable challenges, optimism persists regarding the prospect of establishing a global AI regulatory framework. The potential advantages of such a framework loom large, encompassing enhanced governance, ethical standards, and international cooperation. The growing recognition within the global community of the imperative for collaboration in AI regulation augurs well for concerted efforts towards overcoming the prevailing hurdles.

WHY INTERNATIONAL COOPERATION ON AI IS IMPORTANT

The international AI landscape thrives on collaboration for research, innovation, and standardization. Given the interconnectedness of AI development, regulations must transcend national borders to effectively address the above challenges and ensure ethical practices. Firstly, AI research and development have evolved into complex and resource-intensive endeavours wherein scale plays a pivotal role. Collaborative efforts among governments, AI researchers, and developers across borders can harness the advantages of scale and capitalize on comparative strengths for mutual gain. Without international cooperation, nations may engage in competitive and redundant investments in AI capabilities, incurring unnecessary costs and diminishing overall outcomes. Critical components of AI development, such as access to high-quality data—especially for supervised machine learning—and extensive computing resources, knowledge, and talent, benefit immensely from the scale.

Furthermore, international cooperation founded on shared democratic principles pertaining to responsible AI can steer efforts towards ethical AI development and foster trust. Despite progress in aligning on responsible AI practices, disparities persist, even among participants of forums like the FCAI.[194] The next phase of AI governance entails translating principles into tangible policies, regulatory frameworks, and standards, necessitating a

[193] Legal 500, supra note 110, at 55

[194] The Forum for Cooperation on Artificial Intelligence (FCAI), a collaboration between the Brookings Institution and the Centre for European Policy Studies, hosts regular AI dialogues among high-level officials from seven governments (Australia, Canada, EU, Japan, Singapore, U.K., and the U.S.) as well as experts from industry, civil society, and academia, aimed at identifying opportunities for international cooperation on AI regulation, standards, and research and development. Many of the ideas and policy recommendations from the dialogues are reflected in FCAI reports and blogs.

deeper comprehension of AI's practical implementation and navigating trade-offs inherent in endeavours like balancing accuracy and explainability. Effective cooperation demands specific actions in various domains. Within the AI landscape, different regulatory strategies can create obstacles to innovation and spread. Under the pretence of helping home AI efforts, government actions may have unfavourable effects, like restricting data access, requiring data localization, discriminating investment practices, and other legal requirements. Different risk rating systems and legal requirements might drive up expenses for companies trying to negotiate the international AI market. Different regulatory environments could need customizing AI models to follow different rules, which would increase compliance costs disproportionately for smaller businesses. Discrepant regulations might also engender variations in data collection and storage methodologies, introducing complexity to data systems and diminishing the overall utility of data for AI applications. These additional costs can extend to AI services and hardware-software systems incorporating AI solutions, like autonomous vehicles, robots, or digital medical devices. Facilitating enhanced cooperation is crucial to fostering a broader market wherein nations can leverage their unique competitive advantages. For instance, the European Union through the AI Act aims to establish a competitive edge in "Industrial AI," allowing EU entities to harness AI without necessitating substantial reengineering to meet the requirements of other jurisdictions.

Specialised AI development companies can thrive with coordinated efforts to harmonise important elements of AI regulation. These firms make their money by developing knowledge of certain AI systems and then licencing them to other businesses as parts of larger toolkits. Deeply specialised arrays of AI systems could appear when AI penetrates many industries. Companies would be able to use digital supply chains in a more open global market to include components developed in many locations into their goods. Promoting international rivalry between specialised companies would stimulate markets and advance AI. Furthermore, better trade cooperation is essential to prevent arbitrary limitations on the movement of goods and data, which may severely limit the possible advantages of AI spread. Protectionism, while admitting the strategic significance of data and sovereignty, can stifle international cooperation, upset global value chains, and limit consumer choice, therefore reducing the size of the market and the incentives for significant AI investment. Particularly in areas like data sharing and using AI to battle problems like climate change or pandemic readiness, no country can take on such problems alone. Collaborative endeavours, akin to "moonshots," can pool resources to leverage AI's potential in domains such as healthcare, climate science, or agriculture while serving as platforms for testing responsible AI approaches collectively.

Cooperation among like-minded nations holds significance in reaffirming fundamental principles of openness and safeguarding democracy, freedom of expression, and other human rights. Unrestrained use of AI technologies by techno-authoritarian governments—China being one of them—raises concerns about the possibility of human rights abuses and fragmentation of the global AI R&D scene. The fact that most countries include international cooperation into their AI plans shows that they recognise the close connection between AI advancement and international cooperation.

CONCLUSION

While the AI Act 2024 represents a significant stride towards comprehensive regulation, it also underscores the discussed shortcomings. The act, despite its detailed provisions and ambitious scope, fails to address the full spectrum of challenges posed by AI. The potential Brussels Effect of the Act could lead to a scenario where other nations, including India, are compelled to adapt their own regulations to align with the EU's standards. However, this unilateral approach may not be sufficient to manage the complexities of AI in international trade. The differing regulatory landscapes can result in a fragmented and inconsistent global framework, which not only hinders technological innovation but also complicates the enforcement of AI standards. While adopting similar regulations might provide a pathway for international cooperation, it also highlights the need for a more inclusive and harmonized approach. The disparities in technological advancement and regulatory capabilities among nations necessitate an international agreement that leverages global cooperation to establish a comprehensive and cohesive regulatory framework for AI.

In conclusion, the chapter has exposed that a fragmented and ambiguous regulatory environment poses significant risks to both technological innovation and societal well-being. Therefore, it is imperative for global stakeholders to collaborate and formulate an international regulatory framework that addresses the multifaceted challenges of AI. Only through such concerted efforts can we ensure that AI’s transformative potential is harnessed responsibly and equitably, fostering an environment of trust and innovation in the global marketplace.

CHAPTER 6

CONCLUSION AND RECOMMENDATIONS

Artificial Intelligence, or AI, denotes the replication of human intelligence in machines programmed to think and act like humans. It encompasses machines or software that demonstrate human-like traits in learning and problem-solving. AI's defining feature lies in its capacity to reason and execute actions with the highest probability of achieving specific objectives. The concept of AI is in constant evolution, progressing from its origins in performing calculations to the current capabilities where it autonomously operates vehicles, missiles and even satellites. This evolution has profoundly benefited numerous industries. As artificial intelligence continues to reshape industries and transform the global economy, trade policy must evolve to keep pace and ensure equitable growth for all nations.[195] Regulators and lawmakers worldwide are facing challenges in finding an agreement on suitable regulatory measures for artificial intelligence. Although they have made attempts to keep up with artificial intelligence breakthroughs, their efforts have typically proved insufficient. As a result, regulatory organisations around the world are implementing different approaches to supervise this technology. As a consequence, the global regulatory framework governing artificial intelligence, a transnational technology capable of significantly transforming work patterns, enabling the spread of misinformation, and presenting grave societal hazards, is fragmented and ambiguous. Therefore, it is critical to reach an international agreement, and international cooperation should be utilised to construct a comprehensive global regulatory framework.

WHO SHOULD GOVERN AI GLOBALLY?

From the analysis in the previous chapter, we came to the conclusion that a global AI governance framework is not just advisable but imperative. But who should frame these guidelines? Which international organisation is acceptable worldwide in this regard? These are the further challenges. The preceding chapters discussed the strategies employed by various international organisations such as the OECD, UN, ITU, ISO/IEC, IEEE, G7, and others. However, none of these approaches have garnered universal acceptance, as they were primarily developed to address immediate concerns rather than focusing on long-term

[195] Int’l Inst. for Sustainable Dev., *International Trade and Artificial Intelligence: ChatGPT*, IISD (May 23, 2023), https://www.iisd.org/articles/policy-analysis/international-trade-artificial-intelligence-chatgpt

sustainability and future-oriented solutions. In our view, none of the current endeavours is equipped to effectively regulate AI's potential while simultaneously identifying and mitigating associated risks in isolation. This holds particularly true given the ongoing exploration of AI's capabilities. Comprehending these risks and translating shared principles into action demands thoughtful implementation across diverse scenarios. Such endeavours necessitate engagement from diverse stakeholders, extending beyond governmental entities to encompass private enterprises driving AI innovation and application, as well as a spectrum of other voices. Moreover, these efforts will require time; for example, the establishment of the International Atomic Energy Agency, often cited as a potential model for regulating AI safety, was a multi-decade undertaking involving international agreements.

The United Nations holds a pivotal position in this, yet aiming solely for a unified governing body for global AI management may not be ideal. While the UN plays a vital role due to its capacity to gather a wider number of nations compared to other organisations like the OECD, the G7, GPAI, or temporary coalitions formed by current AI leaders, it also serves as a platform to facilitate access to AI and promote AI development in alignment with the UN Sustainable Development Goals. However, it's crucial that the UN's involvement doesn't overshadow other initiatives, nor should the ultimate objective be a singular governing entity in the foreseeable future. Instead, existing initiatives should run concurrently, guided by the vision set forth by the UN and its member states, with a focus on leveraging AI for the collective benefit of the planet. It should also be kept in mind that even the UN has its own inherent limitations. For instance, while a resolution may establish a global framework, it lacks the power to enforce compliance among member states. Consequently, countries are not obligated to adhere to the guidelines set forth for AI governance or incorporate them into their regional laws merely by the resolution's passage. Nonetheless, the adoption of such a resolution remains significant, as it signifies a widespread consensus on fundamental principles and future trajectories among nations. Furthermore, it exerts pressure on countries opting to disregard the framework, underscoring the importance of collective responsibility in navigating the challenges posed by AI.[196]

Apart from the United Nations, another potential candidate for global governance of Artificial Intelligence is the WTO. As a pioneer in regulating global trade, the WTO wields

[196] Renda, A., Wyckoff, A. W., Kerry, C. F., & Meltzer, J. P, *Should the UN govern global AI?*, Brookings, (February 26, 2024), https://www.brookings.edu/articles/should-the-un-govern-global-ai/

significant influence and implementation power across many countries. Its previous initiatives demonstrate its capability as a global regulator across various domains. For instance, the WTO TBT Agreement, which all WTO members have signed, aims to ensure that technical regulations, standards, and conformity assessment procedures are fair and do not unduly obstruct trade. The agreement strongly promotes the use of international standards to facilitate trade while maintaining the sovereign rights of governments to regulate safety and other essential policies. The TBT agreement promotes a delicate balance between preserving governments' sovereign regulatory rights and minimising unnecessary trade barriers. It strongly advocates the use of international standards to achieve this equilibrium. Further establishing a new forum like a World Technology Organisation, akin to the International Atomic Energy Agency (IAEA), highlighting parallels between AI and nuclear weapons in terms of risks can also be a way forward. However, the creation of an international organisation specifically for AI or technology under any name encounters three significant challenges.

BASIS FOR A GLOBAL FRAMEWORK

In the case of AI, regulation can be said to mean a set of commands, where a set of binding rules are made by the government or any other regulatory agency to deal with any of the issues arising from its use or its effect. However, nations lack consensus regarding the optimal method for regulating AI: should it involve stringent regulations, collaborative regulatory frameworks, accreditation and guarantees, industry norms, or a blend of these approaches? Thus, an international legislative framework is essential to regulating AI. The following should be the basis for good AI regulation.

1. Develop an adaptable and multifaceted framework: The framework should prioritise desired results rather than specific approaches. Rules should be founded on principles and outcomes. Regulations must adapt to technical changes and should not show bias towards specific technology or business models, as they may become outdated and hinder innovation. Instead of inflexible inventories of high-risk technology, regulations should permit adaptable assumptions and give priority to ideals such as equity, openness, and safeguarding. This strategy allows organisations to establish customised internal policies that are suitable for their specific circumstances, while also promoting innovation. Regulatory frameworks should provide guidance without being overly restrictive, allowing regulators to offer

customised advice in a cooperative manner. It is essential to have a comprehensive grasp of the scope of legislation in order to avoid hindering investment and innovation, particularly for small and medium-sized enterprises that are at the forefront of AI progress.

2. Implementing a Risk-Based Approach: Any regulatory policy for AI should strive to protect fundamental human rights and mitigate possible harm to individuals and society, while simultaneously promoting the progress and utilisation of AI for mutual benefit. Abstaining from successful AI technologies may result in risks to individuals and society. This includes the failure to utilise technologies that can detect and prevent diseases, handle online harm, cybersecurity issues, and fraud. A thorough risk-based strategy helps achieve this objective by enabling the implementation of practical preventive measures that are appropriate to the risks and rewards associated with a certain AI system. The primary focus is on understanding the potential consequences of AI technology in certain application scenarios. A risk-based AI regulatory framework would offer organisations flexible criteria for assessing the likelihood and degree of potential harm caused by AI, as well as the necessary steps to mitigate it.

   Organisations can customise their risk mitigation strategies by assessing and understanding the potential consequences of their AI applications, enabling them to avoid unnecessary actions. Furthermore, a risk-based framework should assess the possible advantages of an AI system for individuals, organisations, and society, in comparison to the known hazards linked to implementing (or not implementing) AI. Take self-driving automobiles as an example; the dangers they pose change depending on the conditions they're used in. Perhaps there is less of a risk to people from autonomous vehicles in rural and agricultural areas compared to cities and suburbs. Some benefits of autonomous automobiles in these settings include labour assistance, more sustainable farming methods, and higher yields. When comparing automated vehicles to conventional, human-driven cars, it is crucial to carefully examine the criteria used to assess risk. Instead of using a category approach that labels AI systems as high-risk dangers, a risk assessment-based approach is better.

3. Utilise the current regulations as a foundation: In order to create a flexible and adjustable framework for AI, it is essential to utilise and expand upon current legal systems, which include both explicit legislation (hard laws) and informal guidance (soft law), such as the OECD AI Principles. Many industries have already adopted

stringent rules that spell out specific guidelines for incorporating AI, including healthcare and the financial industry. Still, these rules may need reevaluating and tweaking if we're going to meet the specific problems AI has brought.In order to close regulatory loopholes, specific actions must focus on currently unregulated regions.

Utilising or adhering to the current legal frameworks as a template ensures the establishment of unambiguous and consistent legal standards in a standardised manner. The complexities of AI are influenced by regulations pertaining to consumer safeguarding, intellectual ownership, non-discrimination, data security and confidentiality, and analogous regulations. As an example, the use of personal data by AI is already governed by the EU's General Data Protection Regulation. Addressing the lack of comprehensive federal privacy legislation in the US is crucial for establishing strong regulation of AI. Regulatory organisations can facilitate compliance by providing guidance on the application of current regulations to AI, incorporating input from diverse stakeholders.

It is crucial to acknowledge the necessity of modifying current regulations to accommodate the progress of artificial intelligence. For instance, the criteria outlined in data protection legislation, such as legitimate processing and purpose specification, may clash with the operations of artificial intelligence. Limiting the understanding of these notions could hinder the achievement of AI's positive objectives. Gaining a deeper understanding of the advancement of AI could be beneficial, particularly in terms of redefining the concept of "compatible purposes" and acknowledging algorithmic training as an independent objective. Rigid adherence to data minimization and data preservation requirements might also hinder the learning capabilities of AI. Regulators should engage in collaboration with AI developers and consumers to build interpretations in order to advance and adapt.

It is crucial to include soft law frameworks, industry standards, and co-regulatory instruments produced by stakeholders in existing legislation to ensure their full effectiveness. International standards that define fundamental requirements for the development and implementation of AI are necessary; such standards were deliberated upon during the G7 Summit. The European Union's AI Act is indebted to the OECD AI Principles, an organisation whose mission is to advance international consensus on AI regulations.

4. Ensuring Openness, Equity, Clarity, Safety, and Confidence: To ensure the dependability and beneficial effects of AI, regulations, collaborative efforts, and industry standards are necessary to empower individuals. This can be achieved through:

   Transparency: Developers and users of AI should provide comprehensive and meaningful information about the functioning and data handling of AI systems, while also protecting privacy, data security, and business confidentiality. The general public, auditors, business users, and regulators should all have access to this degree of transparency. The documentation for high-risk AI systems should meticulously detail the intended application, recognised hazards, and strategies to mitigate these risks. It is essential to ensure that clients have a comprehensive understanding of the data practices and constraints associated with generative AI models. This can be achieved via centralised resources, policies, terms of service, notifications, and other channels.

   Explainability: This is a component of transparency that promotes accountability and confidence through the clarification of how AI systems influence outcomes and decisions that affect individuals. Developers and consumers ought to give precedence to the elucidation of AI operations, while also considering the compromises that may arise in the pursuit of explainability. Also, they should address concerns about security, safety, and precision. Attaining complete understanding may be unattainable in specific situations, such as when dealing with intricate language models, due to their intricacy or technical constraints. Organisations must to reveal these trade-offs, particularly when prioritising accuracy over explainability, as is the case in healthcare, where AI can offer significant advantages but may lack complete transparency. Depending on the specific circumstances, requiring full transparency may not be appropriate for every situation.

   Accessibility: Individuals should have easily accessible channels to provide feedback, address grievances, request more information, challenge choices, request human evaluation, and eventually seek resolution if they believe they have been adversely affected by AI. Developers and consumers alike should build end-to-end AI systems with processes for transparency, human review, complaint resolution, and redress to empower and safeguard people.

5. Incorporate demonstrable organisational responsibility: For the purpose of situating accountability within a wider context, regulatory measures should facilitate

organisations in demonstrating their implementation of responsibility frameworks and management initiatives that provide them with the capability to meet all relevant legal requirements and other benchmarks. Similar to conventional corporate compliance and business ethics, and more recently in data, security, and digital domains, accountability should be ingrained and operationalized throughout all phases of the AI lifecycle and its technological infrastructure, encompassing AI datacenter architecture, models, and applications. Looking at current frameworks such as the EU's Risk-Based Framework, Singapore's Model AI Governance Framework, and CIPL's Accountability Framework may teach organisations a lot about how to set up accountability and AI governance programmes.

Organisations are expected to show accountability by all parties involved, whether it be shareholders, investors, regulators, or the general public. Certifications, audits, codes of conduct, and evaluations serve as useful instruments for showcasing accountability. These mechanisms are crucial in digital policy and regulation, particularly for developers and implementers of artificial intelligence, for several reasons: i) They showcase to all stakeholders within the organization a dedication and capability to ensure that products and services adhere to specific standards. ii)They allow firms to turn observable and risk-based controls into principle- and outcome-based legal obligations, improving regulation and compliance. iii) They play a crucial role in establishing legal certainty and enhancing confidence, especially in business-to-business contexts. Every AI policy should clearly state that shown accountability is a key component and make it easier to create and use co-regulatory frameworks that support and demonstrate such accountability, such codes of conduct and certification programmes.

6. Promoting the widespread adoption of responsible AI governance: Apart from requiring a basic package of accountability procedures for organisations involved in the creation and application of artificial intelligence, legislators and regulators should actively promote and reward the use of comprehensive accountability frameworks, tools, and technologies. To make sure that AI is always accountable, the people who are working on these tools and systems need to be closely involved. The goal is to create an environment where companies see strong accountability standards not only as something they have to do by law, but also as a way to make their data operations more valuable and build trust in them. Policymakers and regulators should also grasp the motivations and obstacles related to responsible

technology practices and solutions, such as Privacy Enhancing Technologies (PETs), and take measures to encourage their advancement and wider application.

- ➢ Various incentives can be explored to promote accountability, including: Recognizing demonstrated or certified accountability as a factor in reducing penalties in enforcement actions and determining fines.
- ➢ Thinking of an organization's responsible creation and application of AI models as a "licence to operate," one might give organisations that have put in place robust accountability mechanisms more latitude.
- ➢ Enabling the utilisation of data in AI projects for socially advantageous research, as long as it complies with appropriate risk evaluations.
- ➢ Allowing purchasers of AI systems to fulfil their due diligence obligations by procuring systems certified to recognized standards for responsible AI.
- ➢ Using demonstrated AI accountability as a requirement for eligibility in public procurement projects encourages contractors to seek responsible AI certification.

7. Allocating Liability: Carefully allocate responsibility, prioritizing the party most directly linked to causing harm. Encouraging all participants in the AI ecosystem to adopt mechanisms for organizational accountability can improve adherence to regulations and outcomes, potentially reducing the need for liability disputes. Nevertheless, there are ongoing deliberations on the equitable allocation of liability among the entities engaged in the AI ecosystem.

   In an ideal scenario, the party that is largely responsible for creating the specific injury should bear the blame. However, the process of evaluating liability can be intricate in reality. Precedent, legal requirements, and how pertinent evidence is published will affect this research. In some cases, end users, developers, or both can be held accountable. Developers who misrepresent capabilities or fail to test systems for harm may be liable. There is a possibility that developers could be held legally responsible if they provide misleading information about capabilities or if they do not test systems sufficiently for potential harm. On the other hand, users are also accountable for how they use AI systems, especially if they participate in high-risk activities that go against the recommendations provided by the developers.

   Contracts, particularly the evolving norms of AI contracting, will play a vital role in establishing the obligations and legal liabilities of parties involved in the development and implementation of AI. For instance, if a developer explicitly prohibits a high-risk use case in their product's contract, the user who breaches this agreement should assume the associated risk. Contracts should also specify accountability between model developers and deployers in cases where third parties provide AI models or solutions.

8. Establish mechanisms for coordination and collaboration among regulatory entities:

   8. Establish systems for regulatory agencies to collaborate: AI is omnipresent in many areas, each with its own rules and regulatory bodies. AI-based personal data processing is generally overseen by data protection authorities (DPAs). However, certain regulatory organisations have industry-specific duties. Instead of creating a new AI regulator, which may lead to regulatory redundancy, inconsistency, and legal ambiguity, it is better to improve current regulators' skills and capacities to ensure efficient AI oversight and encourage high-level coordination and cooperation among existing authorities on AI policies.

   A regional central governmental coordination body would be wise to be established, even though it is best for each regulator to keep oversight within their own area (e.g., data protection authorities should keep broad jurisdiction over AI applications that process personal data and have privacy implications). As needed, this organisation would promote regulatory coordination, alignment, and cooperation across regulatory agencies by establishing broad policies and objectives on artificial intelligence that are relevant to different industries. Regulatory agencies would be able to discuss compromises among many policy objectives, such as robustness, efficiency, equity, privacy, and security, on the platform. It would also provide regulators clear direction on the creation and application of artificial intelligence.

   Organisations and regulators alike gain from this strategy since it encourages regulatory consistency and offers thorough, multidisciplinary policy guidance that industries and specialised regulators can use and track more successfully over time. It also helps to harmonise recently passed AI laws and regulations with already in place ones.

   The UK Digital Regulation Cooperation Forum (DRCF), with a permanent CEO and staff, cooperative activities, shared direction, official cooperation projects and staff exchanges, is an example of cross-regulatory collaboration. The DRCF has focused most of its work on AI, as seen by its continuous attempts to increase algorithmic openness. Similar arrangements for regulatory collaboration have been set up in Australia, France, Ireland, and the Netherlands.

9. Facilitate collaborative regulatory oversight and foster ongoing regulatory creativity: Regulators need to improve their skills and strategies in order to negotiate a terrain full with different and occasionally at odds interests. To maintain fundamental rights, data protection authorities could, for example, encourage responsible data use and AI development for societal and economic benefits in addition to protecting individual rights. To be relevant and useful in the digital age, regulatory thinking, priorities, and actions must change. The key to smart and efficient regulation is to approach it risk-oriented. This is understanding the advantages and disadvantages of AI systems and focusing on the areas that pose the greatest risks to people and society while maintaining the advantages of AI. Prioritising their efforts, regulators should concentrate on the areas with the most risk.

   A society powered by technology may find it insufficient to rely just on post-hoc enforcement measures. A cooperative strategy is required, one in which regulators and regulated entities are continuously involved, exchange knowledge and experiences on technology developments, and work together to set reasonable compliance goals. Though enforcement is still a necessary option, investing in proactive accountability measures is probably going to produce greater results than depending just on expensive post-hoc legal action. Using cutting-edge regulatory instruments like policy prototypes and sandboxes, AI may be efficiently supervised. Together with giving regulators more information and practical expertise with AI applications, these tools give the sector a secure environment in which to test ethical innovation under regulatory oversight. Resources should be provided by governments to regulators so they may create and expand these activities, including sector-specific programmes. Regulatory experimentation depends on regulatory sandboxes, which provide a means of applying regulations to novel goods and services under regulatory control. These need to promote creativity and teamwork among interested parties. Likewise, policy prototyping promotes collaboration between public and private organisations, government, business, and academia in the investigation of legislative models prior to passage. In the EU's AI Act, for instance, regulatory sandboxes are proposed; Spain is launching one.[197] A well-established sandbox programme run by the Information Commissioner Office of the United

[197] Bru, P, *Spain legislates for first EU AI Act regulatory sandbox*, Pinsent Masons, (November 17, 2023), https://www.pinsentmasons.com/out-law/news/spain-legislates-for-first-eu-ai-act-regulatory-sandbox

Kingdom also concentrates on biometrics and future technologies. Operating a Data Regulatory Sandbox, Singapore's IMDA offers advice on cutting-edge technologies, including those that improve privacy.[198] Sandbox design should aim to foster creativity while maintaining public confidence and safety.

10. Human Supervision: Tenth, Human Supervision Under human supervision, AI systems are made to respect human autonomy and have no detrimental effects. Particularly with high-risk AI systems, fundamental concepts like justice, security, openness, accountability, and evaluation depend on active human participation. Different systems will require different degrees and kinds of monitoring; there is no universal answer. Rather, as needed, specialised agencies must modify regulations. Systems driven by AI are only as good as human validation and assessment. It takes ongoing observation during the AI system's use to allow for human involvement and to stop operations in the event of a problem.
11. Privacy Concerns: AI driven systems mostly depend on collecting and evaluating a large amount of data on people, their social activities, and other things. Concerns over this procedure, meanwhile, include profiling, selection biases, interference with personal data, and data collecting without consent. These problems emphasise the need of controlling data use in order to protect other people's privacy and to avoid obtaining data without their express permission. The seven fundamental data protection and privacy principles—informed consent, technology neutrality, data controller accountability, data minimization, extensive application, imposition of deterrent penalties, and organised enforcement—should therefore be included into any regulation on AI in order to create strong privacy protection provisions within the laws. Developing operating rules for AI-powered systems according to particular industries or types guarantees a sophisticated solution to related problems. The clauses must to be compliant with worldwide norms for privacy and data protection. In tackling privacy issues associated to AI, this promotes uniformity and enhances international collaboration. Furthermore, severe penalties ought to be applied to AI developers who break the law, encouraging compliance and stressing the value of privacy protection. Promoting AI developers to willingly follow privacy rules fosters a responsible and proactive compliance culture throughout the world.

[198] Press Release, Info-Communications Media Dev. Auth., SG's First GenAI Sandbox for SMEs (June 17, 2024) https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2024/sg-first-genai-sandbox-for-smes

GENERAL SUGGESTIONS

In response to the diverse regional AI legislations emerging globally, it is imperative to formulate a unified global AI regulatory framework. Such a framework would consolidate guidelines and rules essential for governing the complex landscape of artificial intelligence technologies worldwide. This draft framework should encompass comprehensive provisions addressing ethical considerations, accountability frameworks, data privacy standards, and sector-specific implications across various sectors like trade, healthcare, finance, and transportation industries. By establishing a global standard, countries can harmonise their efforts in regulating AI, thereby promoting consistency and clarity in how AI technologies are developed, deployed, and utilized.

Integral to the effectiveness of this global AI regulatory framework is the inclusion of multidisciplinary experts. These experts should span various fields including technology, ethics, law, economics, and policymaking. Their involvement ensures that the regulatory framework meets legal and technical requirements and addresses the broader ethical and societal impacts of AI. By leveraging diverse perspectives, the framework can better navigate the intricate challenges posed by AI technologies, such as bias mitigation, accountability mechanisms, and the ethical implications of automation.

While advocating for regulation at the global level, it is also crucial to acknowledge the need for sector-specific adaptations. A global regulatory framework can establish universal overarching principles and standards for AI technologies. However, allowing for tailored regulations within specific sectors—such as international trade practices—ensures that unique industry dynamics and risks are appropriately addressed. This dual approach of universal standards with sector-specific adaptations strikes a balance between uniformity in core regulatory principles and flexibility in accommodating diverse industry requirements.

Furthermore, harmonising global standards is essential to facilitate interoperability and compliance across borders. International cooperation among regulatory authorities can effectively foster information sharing and collaborative efforts to tackle cross-border AI challenges. Harmonised standards promote innovation and safeguard ethical norms and safety standards universally, ensuring that AI advancements benefit societies globally while minimising risks and disparities. Also, a dynamic regulatory framework should include continuous evaluation and adaptation provisions. Given the rapid pace of technological advancement, ongoing review mechanisms are necessary to update regulations in response to emerging AI capabilities, new risks, and societal feedback. This iterative approach ensures that the regulatory framework remains agile and responsive, capable of fostering innovation while upholding ethical principles and societal values.

In conclusion, policymakers can lay the groundwork for responsible AI development and deployment worldwide by developing a unified global AI regulatory framework supported by multidisciplinary expertise, sector-specific adaptations, harmonised standards, and continuous evaluation mechanisms. Such a framework addresses current regulatory gaps and anticipates future challenges, guiding the ethical and equitable integration of AI technologies into global societies.

BIBLIOGRAPHY

BOOKS

1. Alexander Titus & Adam Russell, The Promise and Peril of Artificial Intelligence -- Violet Teaming Offers a Balanced Path Forward (2023)
2. David Marr, AI: A Personal View, The Foundations of Artificial Intelligence 97, Derek Partridge and Yorick Wilks Edition (2006)
3. Elaine Rich, Kevin Knight & Shivashankar B Nair, Artificial Intelligence 3rd ed. (New Delhi: Tata McGraw Hill India, 2010)
4. European Commission, White Paper on Artificial Intelligence – A European Approach to Excellence and Trust, COM 65 (2020)
5. Nick Bostrom, Superintelligence: Paths, Dangers and Strategies (2014)
6. S. Fiander & N. Blackwood, Robotics and Artificial Intelligence: Fifth Report of Session 2016–17, House of Commons Science and Technology Committee 20 (2016)
7. Stuart J. Russell & Peter Norvig, Artificial Intelligence: A Modern Approach (4th ed. 2021)

REPORTS

1. European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB), Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), (June 18, 2021)
2. Stanford University, Artificial Intelligence Index Report 2023/Chapter 6: Policy and Governance (2023), AI Index
3. Stanford University, Artificial Intelligence and International Trade: Some Preliminary Implications, OECD Trade Policy Papers No. 260 (J. Ferencz, J. López González & I. Oliván García eds., 2022)
4. Stanford University, (2023). *2022 AI Index Report*. Available at: https://aiindex.stanford.edu/wp-content/uploads/2022/03/2022-AI-Index-Report_Master.pdf
5. Report with Recommendations to the Commission of Civil Law Rules on Robotics, Report No A8-0005/2017, European Parliament

6. Georgetown University Center for Security and Emerging Technology, *Artificial Intelligence White Paper 2022* (2022)
7. WTO iLibrary, in Report on AI and International Trade Law, ch. 3 (WTO iLibrary ed., 2023)

ONLINE SOURCES

1. Alessandro Mantelero, Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI, Information Technology and Law Series vol. 36 (Springer-T.M.C. Asser Press 2022), doi:10.1007/978-94-6265-531-7.
2. Artificial Intelligence Act: Council and Parliament Strike a Deal on the First Rules for AI in the World, Council of the EU (Dec. 9, 2023), archived at https://perma.cc/ABC5-XYZW
3. Benjamin Mueller, The Artificial Intelligence Act: A Quick Explainer, Ctr. for Data Innovation (May 4, 2021), archived at https://perma.cc/ABC4-XYZW (Oct. 14, 2022).
4. European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL), doc. no. P8 TA (2017)0051; http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2017-0051&language=EN&ring=A8-2017-0005
5. EU AI Act: First Regulation on Artificial Intelligence, European Parliament News, archived at https://perma.cc/ABC8-XYZW (Jan. 10, 2024).
6. Glenn Greenwald, No Place To Hide: Edward Snowden, The NSA, And The US Surveillance State (Macmillan 2014), https://cis-india.org/internetgovernance/blog/comparison-of-indian-legislation-and-draft-principles-on-surveillanceofcommunications.
7. Hart, Jr. & Todd Eberly Sacks, The Death of the Congressional Committee, Baltimore Sun, http://articles.baltimoresun.com/2011-11-27/news/bs-edsupercommittee-20111127_1_committee-system-committee-chairs-committeehearings/2.
8. Javier Espinoza, EU Agrees Landmark Rules on Artificial Intelligence, Fin. Times (Dec. 9, 2023), archived at https://perma.cc/ABC7-XYZW (Dec. 29, 2023).

9. Jorge Liboreiro, 'Higher Risk, Stricter Rules': EU's New Artificial Intelligence Rules, Euronews (Apr. 21, 2021), archived at https://perma.cc/ABCF-XYZW (Jan. 6, 2024).
10. Luca Bertuzzi, AI Act: EU Policymakers Nail Down Rules on AI Models, Butt Heads on Law Enforcement, Euractiv (Dec. 7, 2023), archived at https://perma.cc/ABCD-XYZW (Jan. 8, 2024)
11. Marcin Szczepański, Economic Impact of Artificial Intelligence, European Parliamentary Research Service, (2019), https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/637967/EPRS_BRI(2019)637967_EN.pdf
12. Mark MacCarthy & Kenneth Propp, Machines Learn That Brussels Writes the Rules: The EU's New AI Regulation, Brookings (May 4, 2021).
13. Martin Coulter, What is the EU AI Act and When Will Regulation Come into Effect?, Reuters (Dec. 7, 2023), archived at https://perma.cc/ABC6-XYZW (Dec. 10, 2023).
14. Michael Veale, Demystifying the Draft EU Artificial Intelligence Act, 22 Computer L. Rev. Int'l 4 (2021), doi:10.31235/osf.io/38p5f.
15. National Program for Artificial Intelligence, UAE Government, https://ai.gov.ae/wp-content/uploads/2020/02/AIGuide_EN_v1-online.pdf.
16. NitiAyog, National Strategy for Artificial Intelligence, 12-17, (2018), https://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-forAI-Discussion-Paper.pdf.
17. N. Nevejans, European Civil Law Rules In Robotics, Directorate General For Internal Policies, Policy Department C: Citizens' Rights And Constitutional Affairs, European Parliament Website, 571 (2017), http://www.europarl.europa.eu.pdf
18. Regulating Chatbots and Deepfakes, mhc.ie (Jan. 9, 2024), archived at https://perma.cc/ABCE-XYZW.
19. Rekha M. Menon, Madhu Vazirani & Pradeep Roy, Rewire for Growth - Accelerating India's Economic Growth for Artificial Intelligence, Accenture Corporation, (2017), https://www.accenture.com/t20171220t030619z__w__/in-en/_acnmedia/pdf-68/accenture-rewire-for-growth-pov-19-12-final.pdf%20-%20zoom=50#:~:text=US%24957%20billion%20to%20India's,extraordinary%20growth%20in%20AI%20investment.

20. S. Moorthy, HTC Global sets sights on education space, (11th December 2019), https://www.thehindubusinessline.com/info-tech/htc-global-setssights-on-education-space/article9989540.ece.
21. The Economic Impact of AI in India, 2020, https://mc.ai/the-economic-impact-of-artificial-intelligence-for-india/.
22. The European Digital Strategy, 2019, https://ec.europa.eu/digital-single-market/.
23. W.A.N.G. Pei, Artificial General Intelligence, Evaluation of AGI Systems, 3, https://www.researchgate.net/publication/26235794 (Aug. 12, 2019).

ARTICLES AND JOURNALS

1. Almada, M., & Radu, A, The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy, SSRN Electronic Journal, (2023)
2. Bradford, A, The Brussels Effect, Oxford University Press, USA (January 1, 2020)
3. Brundage M, The malicious use of artificial intelligence: forecasting, prevention, and mitigation, (2018)
4. Charlotte Siegmann and Markus Anderljung, The Brussels Effect and Artificial Intelligence: How EU Regulation Will Impact the Global AI Market, Centre for the Governance of AI, (August 16, 2022)
5. Daniel Cullen, Why Artificial Intelligence Is Already a Human Rights Issue, Oxford Human Rights Hub (2018)
6. Engler, A, The EU AI Act will have global impact, but a limited Brussels Effect, Brookings (June 8, 2022)
7. EU Artificial Intelligence Act. (n.d.)., High-level summary of the AI Act (2024)
8. European Commission, Policy and Investment Recommendations for Trustworthy Artificial Intelligence, Digital Single Market, https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence
9. European Union, General Purpose AI and the AI Act: A First Look (May 2022)
10. Executive Office of the President National Science and Technology Council Committee on Technology, Preparing For The Future of Artificial Intelligence (2016)
11. Ford, C., Nietsche, C., & Tar, J, US-EU AI Code of Conduct: First Step Towards Transatlantic Pillar of Global AI Governance (July 27, 2023)
12. Franks, E., Lee, B., & Xu, H.. Report: China’s New AI Regulations, Global Privacy Law Review, 5 (Issue 1), 43–49 (March 1, 2024)

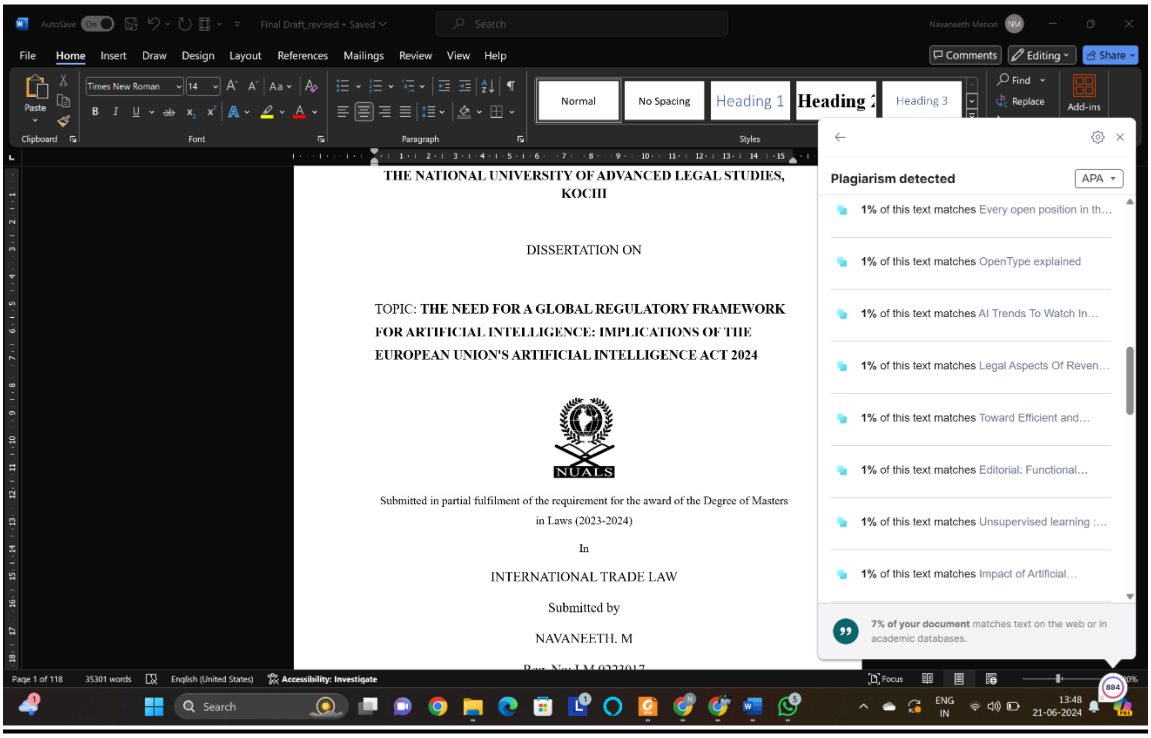
13. Full Translation: China’s “New Generation Artificial Intelligence Development Plan” (2017) - DigiChina. (October 1, 2021)
14. George F. Luger & William A. Stubblefield, Defense Science Board, Artificial Intelligence: Structures and Strategies for Complex Problem Solving (6th ed. 2008).
15. Gluyas L, Day S, Artificial Intelligence - Who Is Liable When AI Fails To Perform? CMS Cameron McKenna Nabarro Olswang LLP (2018)
16. Information Commissioner's Office (ICO), Big data, artificial intelligence, machine learning and data protection, Version: 2.2, 2017
17. International Bar Association Global Employment Institute, Artificial Intelligence and Robotics and Their Impact on the Workplace (2017).
18. IT Exchange, AI Regulatory Initiatives Around the World: An Overview, IT Exchange (2023)
19. ITU Telecommunication Development Sector, Digital Agriculture: Harnessing the Power of AI for Agriculture, (2020)
20. India Briefing, India: Regulation of AI and Large Language Models, INDIA BRIEFING (June 13, 2024)
21. LDP Headquarters for the Promotion of Digital Society Project Team on the Evolution and Implementation of Ais, The AI White Paper Japan's National Strategy in the New Era of AI, April 2023
22. Lennart S. Lutz, Automated Vehicles in the EU: A Look at Regulations and Amendments, GENRE, 12, (March 10, 2018)
23. Miao, F., Holmes, W., Huang, R., Zhang, H., & U, AI and education, UNESCO Publishing, (April 8, 2021)
24. Melanie Arntz, Terry Gregory & Ulrich Zierahn, The Risk of Automation for Jobs in OECD Countries: A Comparative Analysis, OECD Social, Employment, and Migration Working Papers No. 189 (2016).
25. Matthew U. Scherer, Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies, 29 Harv. J. L. & Tech. 353 (2016)
26. Musch, S., Borrelli, M., & Kerrigan, C, The EU AI Act As Global Artificial Intelligence Regulation, SSRN Electronic Journal (2023)
27. NIST, AI Risk Management Framework (January 5, 2024)
28. Paolucci, F, Shortcomings of the AI Act: Evaluating the New Standards to Ensure the Effective Protection of Fundamental Rights, Verfassungsblog (March 14, 2024)

29. Paolucci, F, Shortcomings of the AI Act: Evaluating the New Standards to Ensure the Effective Protection of Fundamental Rights, Verfassungsblog (March 14, 2024)
30. Patrick Henry Winston, Artificial Intelligence (3rd ed. 1992)
31. Renda, A., Wyckoff, A. W., Kerry, C. F., & Meltzer, J. P, Should the UN govern global AI?, Brookings, (February 26, 2024)
32. Stuart J. Russell & Peter Norvig, Artificial Intelligence: A Modern Approach (4th ed. 2021)
33. S Gardner, AI poses big privacy and data protection challenges, Bloomberg Law News, (2016)
34. Tanya Roay, The History and Evolution of Artificial Intelligence; AI's Present and Future, All Tech Magazine, (2023)
35. UK Government, Department for Digital, Culture, Media & Sport, A Pro-Innovation Approach to AI Regulation.
36. United Nations Interregional Crime and Justice Research Institute (UNICRI), AI Against Crime: Leveraging Artificial Intelligence and Machine Learning to Fight Crime, (2020)
37. Victor M. Palace, What If Artificial Intelligence Wrote This: Artificial Intelligence and Copyright Law, 71 Fla. L. Rev. 217 (2019)
38. Willick, M. S, Artificial Intelligence: Some Legal Approaches And Implications, 5 (AI MAGAZINE 2017)
39. Woodrow Barfield & Ugo Pagallo, Research Handbook on the Law of Artificial Intelligence, Edward Elgar Publishing, (2018)

PLAGIARISM REPORT

1.	NAME OF CANDIDATE	NAVANEETH. M
2.	TITLE OF DISSERTATION	THE NEED FOR A GLOBAL REGULATORY FRAMEWORK FOR ARTIFICIAL INTELLIGENCE: IMPLICATIONS OF THE EUROPEAN UNION'S ARTIFICIAL INTELLIGENCE ACT 2024
3.	NAME OF THE SUPERVISOR	Dr. ATHIRA P. S
4.	SIMILAR CONTENT IDENTIFIED (IN PERCENTAGE)	7%
5.	ACCEPTABLE MAXIMUM LIMIT	10%
6.	SOFTWARE USED	GRAMMARLY
7.	DATE OF VERIFICATION	21.06.2024

NAME AND SIGNATURE OF THE CANDIDATE	NAVANEETH. M
NAME AND SIGNATURE OF THE SUPERVISOR	Dr. ATHIRA P. S



THE NATIONAL UNIVERSITY OF ADVANCED LEGAL STUDIES, KOCHI

DISSERTATION ON

TOPIC: **THE NEED FOR A GLOBAL REGULATORY FRAMEWORK FOR ARTIFICIAL INTELLIGENCE: IMPLICATIONS OF THE EUROPEAN UNION'S ARTIFICIAL INTELLIGENCE ACT 2024**

NUALS

Submitted in partial fulfilment of the requirement for the award of the Degree of Masters in Laws (2023-2024)

In

INTERNATIONAL TRADE LAW

Submitted by

NAVANEETH. M

Plagiarism detected APA

1% of this text matches Every open position in th…

1% of this text matches OpenType explained

1% of this text matches AI Trends To Watch In…

1% of this text matches Legal Aspects Of Reven…

1% of this text matches Toward Efficient and…

1% of this text matches Editorial: Functional…

1% of this text matches Unsupervised learning :…

1% of this text matches Impact of Artificial…

7% of your document matches text on the web or in academic databases.

Page 1 of 118 35301 words English (United States) Accessibility: Investigate