



HAL
open science

Defining AI Systems in the EU and Beyond: Assessing the Global Outreach of the AI Act's Norms

Theodoros Karathanasis

► **To cite this version:**

Theodoros Karathanasis. Defining AI Systems in the EU and Beyond: Assessing the Global Outreach of the AI Act's Norms. 2024. hal-04844936

HAL Id: hal-04844936

<https://hal.univ-grenoble-alpes.fr/hal-04844936v1>

Submitted on 18 Dec 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

Assessing the Global Outreach of the AI Act's Norms

Theodoros Karathanasis¹

Abstract: The aim of this working document is to assess the global reach of the European Union's regulatory influence on AI. Based on the final version of the EU AI Act, the analysis in this document focuses on how AI systems are defined and presents the hypothesis that the more rigid the definition of AI systems is, the less global the reach of the EU AI Act's standards will be, especially in states with a strong tendency towards AI sovereignty. A qualitative comparative analysis of four case studies (Brazil, Canada, Chile, USA) reveals persistent divergences between the two sides of the Atlantic regarding how AI and AI systems are defined. Since the main divergence in definitions is centred on the material scope of AI systems, the preliminary conclusion is that the global outreach of the EU AI Act is likely to be unsuccessful in the long term.

Keywords: AI Systems, Regulation, AI Sovereignty, EU Law, Global Norms

Introduction

The AI act mandates that any provider or deployer of an AI system must comply with the AI Act, regardless of where they are located², if “*the output produced by the system is intended to be used*” in the EU (its extraterritorial application). This provision implies that providers situated outside the EU will have to comply with a set of requirements, if they want their products to gain access to the European market.

This requirement reflects to some extent the ‘critical goal of the AIA to set a worldwide standard’³ through what is called the “Brussels Effect”⁴, which means that the attractiveness of the EU's single market may induce companies to follow strict EU standards in their global operations, while other jurisdictions may model their own rules on the EU approach. However, it is believed that the global reach of EU policy in relation to AI may be reduced as a result.⁵ How AI systems are defined in the AI Act may however have significant economic, political, and technological implications for the EU, since the scope of the EU’s AI rulebook will also be defined. According to recent research conducted by Tervel Bobev, Researcher at the Centre for IT & IP Law, it seems that the definition of AI systems remains vague, which has raised concerns about the AI Act being implemented effectively.⁶

¹ Dr. Theodoros Karathanasis, University of Grenoble Alpes (FR) – Chair on Legal and Regulatory Implications of Artificial Intelligence. This work has been partially supported by MIAI @ Grenoble Alpes, (ANR-19-P3IA-0003) and by the Interdisciplinary Project on Privacy (IPoP) commissioned by the Cybersecurity PEPR (ANR 22-PECY-0002 IPOP). ORCID 0000-0002-9645-9312.

² Article 2 AI Act

³ Engler A. ‘The EU AI Act will have global impact, but a limited Brussels Effect’, Brookings, 8 June 2022.

⁴ See Bradford A. (2020) ‘The Brussels Effect: how the European union rules the world’ (Oxford: Oxford University Press).

⁵ See Almada M, Radu A. The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy. German Law Journal. Published online 2024:1-18. doi:10.1017/glj.2023.108; Engler A. ‘The EU AI Act will have global impact, but a limited Brussels Effect’, Brookings, 8 June 2022.

⁶ Bobev T. Defining AI in the AI Act: Pin the Tail on the System. Ku Leuven CiTiP Blog, 2 April 2024. Available at https://www.law.kuleuven.be/citip/blog/defining-ai-in-the-ai-act-pin-the-tail-on-the-system/?utm_source=stack&utm_medium=email (Last accessed 4 July 2024).

In the final version of the AI Act signed by the President of the European Parliament and the President of the Council, and published in June, an AI system is defined as “*a machine-based system that is 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*”.⁷ However, most countries around the world have implicitly defined AI systems as a means of applying the abilities of AI.

Drawing from Bobev’s research on the ‘vagueness’⁸ of the AI Act’s definition of AI systems and the inconsistency in definition between the majority of countries, this working document aims to test the hypothesis that the more rigid the definition of AI systems, the less global the reach of the standards of the EU AI Act will be in states with a strong tendency towards AI sovereignty. The first section of this document presents the concept of AI sovereignty (1.), while the second section puts forward the methodology used to evaluate this hypothesis (2.). The third section presents the regulatory approach adopted by the selected case studies by looking at proposals or adopted legislation currently under discussion (3.).

I. The concept of ‘AI Sovereignty’

Benjamin Cedric Larsen, AI and Machine Learning Project Lead at the World Economic Forum’s Centre for the Fourth Industrial Revolution, states in his article entitled “The geopolitics of AI and the rise of digital sovereignty”: *‘Growing mistrust between nations (...) has caused a rise in digital sovereignty, which refers to a nation’s ability to control its digital destiny and may include control over the entire AI supply chain, from data to hardware and software’*.⁹

In order to describe the AI-specific aspects of digital sovereignty as effectively as possible, scholars are resorting to the not universally defined concept of AI Sovereignty.¹⁰ In fact, three definitions of AI Sovereignty have been proposed. Mügge defines it as “*the need for control, as necessary to develop and deploy AI technologies, of computing capacity and data storage, of access to human resources and potentially proprietary knowledge to build AI applications, and of training data*”.¹¹ Belli considers AI Sovereignty to be “*the capacity of a given country to understand, develop and regulate AI systems*” as long as it is “*essential to retain control, agency, and self-determination over AI systems*”.¹² While Calderaro & Blumfelde describes it as “*the sovereignty over its core intrinsic elements, i.e. data, algorithms*

⁷ PE-CONS 24/1/24 REV 1, Brussels, 13 June 2024

⁸ Bobev T. Defining AI in the AI Act: Pin the Tail on the System. Ku Leuven CiTiP Blog, 2 April 2024.

⁹ Larsen, B. (2022) ‘The geopolitics of AI and the rise of digital sovereignty’, Brookings Institution.

¹⁰ See Mügge, D. (2024). EU AI sovereignty: for whom, to what end, and to whose benefit? *Journal of European Public Policy*, 1–26; Belli, L. (2023) ‘To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE)’, *New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms*, ed. Steven Feldstein. Washington, DC: Carnegie Endowment for International Peace; Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: the false promise of digital sovereignty. *European Security*, 31(3), 415–434.

¹¹ See Mügge, D. (2024). EU AI sovereignty: for whom, to what end, and to whose benefit? *Journal of European Public Policy*, 1–26.

¹² Belli, L. (2023) ‘To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE)’, *New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms*, ed. Steven Feldstein. Washington, DC: Carnegie Endowment for International Peace.

and hardware”,¹³ since control over digital technologies (including AI) is essential for a nation's security, economic prosperity, and autonomy in the globalised world.

For the purposes of this article, I have chosen to use Belli's definition of the concept of AI Sovereignty, as the “*the capacity of a given country to understand, develop and regulate AI systems*” encapsulates the three criteria, and this will allow me to evaluate the tendency of third countries toward AI Sovereignty and therefore, facilitate the selection of the case studies and the assessment of the retained hypothesis.

II. Methodology

Measuring the tendency of third countries toward AI Sovereignty requires referencing the 2023 Government AI Readiness Index provided by Oxford Insights.¹⁴ The purpose of this research work is to provide insights from 2020 about the readiness of government to implement AI in the delivery of public services to their citizens. The research used 39 indicators across 10 dimensions, and involves 3 pillars: Government, the Technology Sector, and Data & Infrastructure.

Even though the issue addressed by the authors by means of this index is not related to the present article research topic, these three pillars allow us to evaluate the tendency of third countries toward AI Sovereignty, whether a given country's effort to understand, develop and regulate AI systems is aimed toward the implementation of AI in the delivery of public services to its citizens or not.

According to the authors, the Government pillar was linked to a state's strategic vision in terms of “*how it develops and governs AI, supported by appropriate regulation and attention to ethical risks (governance and ethics)*” and by its internal digital capacity, which includes “*the skills and practices that support its adaptability in the face of new technologies*”.¹⁵ Regarding the Technology Sector pillar, the maturity, innovation capacity and human capital of the sector were considered. The Data & Infrastructure pillar included the data availability, data representativeness and infrastructure “*necessary to power AI tools and deliver them to citizens*”. Based on the index data delivered with the report, I have come up with 166 countries after excluding the Member States of the EU from the ranking list.

Given that the hypothesis tested in this article was linked to the global reach of the EU AI Act's standards against third countries' tendency toward AI Sovereignty and therefore, their willingness to also export their own standards, it was necessary to also consider, when selecting the case studies, the fact that most international countries have not set standards in the midst of a national legal framework that has already been established. Some states are at the stage of publishing soft-law instruments (strategies, recommendations, guidelines),¹⁶ while others are continuing to put their bills through the legislative process.

¹³ Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: the false promise of digital sovereignty. *European Security*, 31(3), 415–434.

¹⁴ This report is available at <https://oxfordinsights.com/wp-content/uploads/2023/12/2023-Government-AI-Readiness-Index-2.pdf> (Last accessed 4 July 2024).

¹⁵ It should be stressed that the EU AI Act draws from the term digital literacy by using the term AI literacy. The term is understood as “skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause” (Article 3, point 56). Regarding digital literacy, see Gilster, P. (1997) ‘Digital literacy’ (New York: Wiley), p.12. See also Podgorny, B., & Volokhova, N. (2021). Digital Literacy Of The Population: Regional Features. In E. Popov, V. Barkhatov, V. D. Pham, & D. Pletnev (Eds.), *Competitiveness and the Development of Socio-Economic Systems*, vol 105. European Proceedings of Social and Behavioural Sciences (pp. 696-707). European Publisher.

¹⁶ See literature on soft law: Fukui, Y. (2024) ‘International Nuclear Security Law: The Use of ‘Soft Law’’, *Journal of Conflict and Security Law*, 29:(1) 129–142; Elgesem, F. (2024) ‘The Role of Soft Law in the Application of the Law: The Norwegian Perspective’, *Oslo Law Review*, 2:(10) 1–8; Evans, M. D. (2014) ‘International law

Therefore, based on IAPP's 2024 Global AI Law and Policy Tracker¹⁷, which identifies legislative and/or policy developments in a subset of jurisdictions, the selected pool of 166 countries was reduced to 12 countries.¹⁸ Of these 12 countries only 4 were retained (Brazil, Canada, Chile and the United States of America) as they are discussing a bill or have already adopted a national law. The rest of the potential case studies were excluded as these countries do not yet have a specific AI Act or bill; there was neither a bill released following a national legislative procedure nor an Act adopted (i.e. UK, New Zealand).¹⁹ Moreover, bills may have been planned by the government, but they had not been released at the time of writing (i.e. India,²⁰ Israel,²¹ Taiwan).²² Lastly, there were a couple of cases where it was not possible to find the bill to assess its content (i.e. China,²³ South Korea).²⁴

The next step toward assessing this hypothesis was to evaluate the rigidity of the definition of AI systems included in the final AI Act, as the AI Act aims to ensure that international companies comply with European rules while strengthening the EU's resolve to secure AI sovereignty. Following a series of long debates that have taken place since 2021, the EU's Ordinary Legislative Process (COD) concerning the Commission's proposal for an EU AI Act went a step further, with the European Parliament endorsing a first reading of the AI Act during its plenary session in Strasbourg, with 523 votes in favor, 46 against and 49 abstentions.²⁵ Due to the extensive nature of the amendments to the Commission's proposal for an AI Act, the text adopted by the EP had to be further scrutinised and revised by legal experts, in accordance with Rule 181 of the EP's Rules of Procedure,²⁶ in order to ensure linguistic precision and legal consistency before it became law.

Drawing from the definition of an AI system in Article 3(1) of the AI Act, six comparative criteria were retained: (a) machine-based system, (b) varying levels of autonomy, (c) adaptiveness after deployment,

(Fourth edition)', Oxford University Press; Oxford; Van der Sluijs, J. (2013) 'Soft law: an International Concept in a National Context', *Scandinavian Studies in Law*, 58 285-306; Guzman, A. T. & Meyer, T. L. (2010) 'International Soft Law', *Journal of Legal Analysis*, 1:(2) 171-225;

¹⁷ See IAPP Research and Insights, 'Global AI Law and Policy Tracker', Last updated in February 2024 - <https://iapp.org/resources/article/global-ai-legislation-tracker/> (Last accessed 4 July 2024).

¹⁸ Brazil, Canada, Chile, China, Israel, India, New Zealand, South Korea, Taiwan, UK and the USA.

¹⁹ The only AI-specific policy is the Algorithm Charter, which most government agencies have signed up to. Signatories to the Algorithm Charter have agreed to apply certain principles in how they use algorithms, especially in designing access to public services but it doesn't address newer technologies such as the LLMs. However, the document does not contain a definition for AI or AI systems.

²⁰ Advocating for a robust, citizen-centric and inclusive "AI for all" environment, India government proposed a Digital India Act that would replace the IT Act of 2000 and regulate high-risk AI systems. India was looking to release the first draft of the Digital India Bill by the end of July 2023, it is deemed however unlikely to be done before 2024 general elections.

²¹ For the time being, Israel has chosen to forget formal AI legislation.

²² In Taiwan, the Executive Yuan originally planned to draft Artificial Intelligence Basic Law in September 2023. However, after taking into account the recent developments in generative AI technologies, the launch of the draft is postponed to 2024.

²³ China's approach to AI legislation is evolving rapidly and is heavily based on central government guidance. On May 10, 2024, the Ministry of Industry and Information Technology of the People's Republic of China (MIIT) published a notice of the General Office of the State Council on the issuance of the 'State Council 2024 Legislative Work Plan'. In particular, the MIIT outlines, among other things, that the draft Artificial Intelligence Law was prepared to be submitted to the Standing Committee of the National People's Congress for review. Source: <https://www.dataguidance.com/news/-miit-includes-draft-ai-law-state-council-2024> (Last accessed 4 July 2024).

²⁴ The Science, ICT, Broadcasting and Communications Committee of Korean National Assembly passed on February 14, 2023, a proposal to enact "Act on Promotion of AI Industry and Framework for Establishing Trustworthy AI" (the "AI Act"). While the specifics remain to be determined, this legislation diverges from the EU's AI Act by embracing the principle of "embracing technology before regulation," with the goal of fostering the advancement and industrial implementation of AI technologies.

²⁵ European Parliament, Agenda for the European Parliament's plenary sessions of 11 - 14 March 2024 in Strasbourg.

²⁶ Admissibility of amendments

(d) generates output, (e) explicit or implicit objectives and (d) physical/virtual environments. The choice of these criteria stems from the fact that they depict the evolution of the definition, during the COD regarding the adoption of the AI Act (**Table 2**).

Table 2. The Evolution of the Definition of the notion of ‘AI Systems’: from the AI Act Proposal to its Final Version (wording)						
Criteria/Institutions	Machine-based system	Human in/on the loop	Adaptive-ness	Generates output	Explicit or implicit objectives	Physical/virtual environments
Commission Proposal	<i>Software</i>	<i>Techniques and approaches listed in Annex I</i>	-	<i>Generates output</i>	<i>Human-defined objectives</i>	<i>Environments</i>
Council Position	<i>System based on machine and/or human-provided data and inputs</i>	<i>Elements of autonomy</i>	-	<i>System generated output</i>	<i>Given set objectives</i>	<i>Environments</i>
EP Position	<i>Machine-based system</i>	<i>Varying levels of autonomy</i>		<i>Generates output</i>	<i>Explicit or implicit objectives</i>	<i>Physical/virtual environments</i>
Finalized AI Act	<i>Machine-based system</i>	<i>Varying levels of autonomy</i>	<i>Adaptive-ness</i>	<i>Generates output</i>	<i>Explicit or implicit objectives</i>	<i>Physical/virtual environments</i>

Table produced by author

According to recital 12 of the final version of the AI Act, the six retained criteria should be understood as follows:

- a) **Machine-based system:** The term “machine-based” is defined in the AI Act as an AI system that “*runs on machines*”.²⁷ However, according to the OECD Explanatory Memorandum on the Updated OECD Definition of an AI System, an AI system is “*typically built by combining one or more models developed manually or automatically (e.g., with reasoning and decision-making algorithms) based on machine and/or human inputs/data*”.²⁸ In the Council’s General Approach document concerning the AI Act, it was explicitly mentioned that an AI system is, amongst other things, ‘*based on machine and/or human-provided data and inputs*’. Moreover, in the Commission’s communication on “Artificial Intelligence for Europe” of 2018,²⁹ it was clearly stated that “*AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)*”.³⁰ An approach that was also shared to some extent by the Commission’s High-Level Expert Group on AI (HLEG-AI), as it retained the following definition of an AI system: “*any AI-based component, software and/or hardware. Indeed, usually AI systems are embedded as components of larger systems, rather than stand-alone systems*”.³¹ I argue that the purpose of

²⁷ Recital 12 of the AI Act.

²⁸ OECD (2024), Explanatory Memorandum on the Updated OECD Definition of an AI System, p. 8

²⁹ European Commission (2018) Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, Brussels, 25.4.2018 COM(2018) 237 final.

³⁰ COM(2018) 237 final, p. 1

³¹ HLEG-AI (2018), A Definition of AI: Main Capabilities and Scientific Disciplines - Definition developed for the purpose of the deliverables of the High-Level Expert Group on AI, Brussels, 18 December 2018.

retaining the term “machine-based” to define an AI system, was probably due to seeking to distinguish it from AI models, for which a distinct set of obligations applies under the AI Act.

- b) **Human on/in the Loop:** In the OECD’s Explanatory Memorandum, the autonomy of an AI is understood as “*the degree to which a system can learn or act without human involvement following the delegation of autonomy and process automation by humans*”.³² The key term here is “human involvement”, which can also be found in Recital 12 of the AI Act.³³ However, the EU lawmakers went further by including the term ‘human intervention’. Indeed, Recital 12 states that “*AI systems are designed to operate with varying levels of autonomy, meaning that they have some degree of independence of actions from human involvement and of capabilities to operate without human intervention*”. Published in 2019, the European Commission’s “Ethics Guidelines for Trustworthy AI” introduced the concepts of “human in the loop” - the extent of human intervention and “human on the loop” - the extent to which the overall activity can be overseen.³⁴
- c) **Adaptiveness:** Adaptiveness is “*usually related to AI systems based on machine learning that can continue to evolve after initial development*”.³⁵ In other words, the system adjusts its behaviour by directly interacting with input and data, either before or after deployment. The AI Act’s approach toward adaptiveness seems to be in line with this definition, as Recital 12 states that adaptiveness refers to “*self-learning capabilities*” that an AI system could “*exhibit after deployment*”, therefore “*allowing the system to change while in use*”. The concept of adaptiveness often relates to what experts call emergent AI abilities,³⁶ which is understood as the ability of a machine to perceive and respond to the changing environment around it, adapting and learning automatically from large volumes of information.
- d) **Generation of an output:** Outputs generally reflect different tasks or functions performed by AI systems. The OECD is formulating a non-limitative list of such outputs (recognition, event detection, forecasting, personalisation, interaction support, goal-driven optimisation, reasoning with knowledge structures etc...).³⁷ The term “such as” retained in the definition of AI systems in the AI Act indicates that there may also be outputs other than ‘*predictions, content, recommendations, or decisions*’. Indeed, Recital 12 of the AI Act specifies that “*The reference to predictions includes content, which is considered in this Regulation a form of prediction as one of the possible outputs produced by an AI system*”.
- e) **Explicit or implicit objectives:** In the OECD’s Explanatory Memorandum³⁸, which clarifies the definition of an AI system contained in the 2019 OECD Recommendation on AI,³⁹ it is stated that an AI system’s explicit or implicit objectives can refer to the following categories, which may overlap in some systems:

³² OECD (2024), Explanatory Memorandum on the Updated OECD Definition of an AI System, p. 6

³³ It should be stressed that in the EU, the GDPR introduced the notion of ‘human intervention’ as a way of preventing, in certain circumstances, decision-making based solely on automated means. It could be then argued that the inclusion of the term ‘human intervention’ stems from the willing of the EU lawmakers to establish a kind of “conformity” with the GDPR requirements. See Article 22 of the GDPR.

³⁴ HLEG (2019) Ethics Guidelines for Trustworthy AI.

³⁵ OECD (2024), Explanatory Memorandum on the Updated OECD Definition of an AI System, p. 6

³⁶ Regarding emergent abilities of AI, see: Bereczki, T. & Ádám Liber (2023), ‘AI’s emergent abilities a “double-edged sword”, IAPP news, 11 October 2023.

³⁷ OECD (2022), OECD Framework for the Classification of AI systems, OECD Publishing.

³⁸ OECD (2024), Explanatory Memorandum on the Updated OECD Definition of an AI System, DSTI/CDEP/AIGO(2023)8/FINAL.

³⁹ OECD (2019), Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449.

- i) *Explicit and human-defined* – where the developer encodes the objective directly into the system (e.g., through an objective function).⁴⁰
- ii) *Implicit in (typically human-specified) rules*: rules dictate the action to be taken by the AI system according to the current circumstance.⁴¹
- iii) *Implicit in training data*: where the ultimate objective is not explicitly programmed but incorporated through training data and a system architecture that learns to emulate those data (e.g., rewarding large language models for generating a plausible response).
- iv) *Not fully known in advance*: some examples include recommender systems that use reinforcement learning to gradually narrow down a model of individual users’ preferences.

The AI Act follows the same approach by only making reference to ‘explicit or implicit objectives’ and details this criterion further using sub-categories. However, it clearly acknowledges that ‘*these objectives may be “different from the intended purpose of the AI system in a specific context”*’, which is linked to the adaptiveness and thus the emergent abilities of an AI system. I therefore came to the conclusion that such a description encompasses, based on a thorough reading of the AI Act’s definition, all four categories listed by the OECD (explicit and human defined, implicit in human-specified rules or in training data, not fully known in advance). Therefore, all four categories listed by the OECD⁴² will be taken into account when assessing this criterion in relation to third countries’ definition of an AI system.

- f) **Physical/virtual environment**: According to the OECD, “*an environment or context in relation to an AI system is an observable or partially observable space perceived using data and sensor inputs and influenced through actions (through actuators)*”. Moreover, such an environment “*influenced by AI systems can be physical or virtual and include environments describing aspects of human activity, such as biological signals or human behaviour*”. On the other hand, Recital 12 of the AI Act states that “*environments should be understood to be the contexts in which the AI systems operate, whereas outputs generated by the AI system reflect different functions performed by AI systems and include predictions, content, recommendations or decisions*”. Both approaches discuss the relationship between AI systems and their environments, but they differ in their emphasis and scope. The first approach focuses on the technical aspects of the environment, describing it as the space perceived by the AI system through data and sensor inputs, and influenced by the system's actions through actuators. The second approach, on the other hand, is more regulatory in nature. It defines environments as the contexts in which AI systems operate, distinguishing the inputs received by the AI system from its environment and the outputs generated by the AI system based on those inputs. It also highlights the fact that the outputs of the AI system can further influence the environment, even if this just involves introducing new information. Conceptually, while both approaches acknowledge the interaction between AI systems and their environments, the first approach delves into the technical aspects of this interaction, while the second approach provides a regulatory perspective, emphasising the importance of understanding and regulating the impact of AI systems on their environments.

⁴⁰ Examples of systems with explicit objectives include simple classifiers, game-playing systems, reinforcement learning systems, combinatorial problem-solving systems, planning algorithms, and dynamic programming algorithms.

⁴¹ For example, a driving system might have a rule “If the traffic light is red, stop.” However, these systems’ underlying objectives, such as compliance with the law or avoiding accidents, are not explicit, even though they are typically human-specified.

⁴² OECD (2024), Explanatory Memorandum on the Updated OECD Definition of an AI System, p. 7

Overall, these six criteria were retained in order to assess the “rigidity” of the EU AI Act’s definition of AI systems comparatively and qualitatively in relation to the selected case studies.

III. The Case studies’ Hard Law Approach toward AI Regulation

Indeed, in the case of the **EU**, AI Sovereignty is not only expressed via “*more self-reliance on things like hardware and supply chains*”⁴³ but also through ‘*beefing up the regulatory framework*’.⁴⁴ Notwithstanding the Council’s final endorsement in May, the EU AI Act represents the first comprehensive legal framework on AI worldwide. The aim of the new rules is to foster trustworthy AI in Europe and beyond, by ensuring that AI systems respect fundamental rights, safety, and ethical principles and by addressing the risks posed by very powerful and impactful AI models.

The **United States**, despite boasting a vast technology sector and a rich legacy of pioneering AI research, has opted for a decentralised approach to AI, and essentially established a ‘default policy of non-regulation’ until the end of 2023.⁴⁵ On October 30, 2023, the Biden Administration released an Executive Order (E.O.) on “*Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*”.⁴⁶ While the AI Act presents a risk-based regulatory framework, classifying AI systems according to their level of risk (with stricter rules for higher risk and certain forbidden uses of AI), Joe Biden’s EO aims to ensure responsible innovation by focusing on standards and guidelines. The definition in the document emphasises the ability of AI systems to learn from data and achieve specific objectives without human intervention. It also emphasises that the use of machine learning models and other computational architectures is the foundation of AI systems.

Regarding **Canada**, in June 2022 the Government of Canada tabled the Artificial Intelligence and Data Act (AIDA) as part of Bill C-27. In the AIDA proposal, an AI system is defined as ‘a technological system that, autonomously or partly autonomously, processes data related to human activities through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions’. Although AIDA and the AI Act take similar approaches to categorising high-risk systems, the obligations imposed on individuals who design, develop, or otherwise make those systems available are not entirely the same.

In **South America**, the rapid advance and adoption of AI in various sectors of society led the **Brazilian** Government to take regulatory measures. Following the launch of the 2021 Brazilian Strategy for Artificial Intelligence (EBIA),⁴⁷ the Commission of Jurists (CJSUBIA), prepared a final report upon completion of the committee’s work, which included a draft bill that was converted into Bill n° 2338/2023.⁴⁸ The aim of the proposal, which has been discussed in the Brazilian Congress since May 2023, is to help protect citizens’ rights, promote fairness, and prevent discrimination and other potential risks, thus

⁴³ Creemers R. ‘The Chinese Approach to Digital Sovereignty: 4 Questions To Rogier Creemers’, Interview, Sciences Po, 5 April 2023

⁴⁴ Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: the false promise of digital sovereignty. *European Security*, 31(3), 415–434.

⁴⁵ Woods, Andrew Keane, ‘Digital Sovereignty + Artificial Intelligence’, Anupam Chander, and Haochen Sun (eds), *Data Sovereignty: From the Digital Silk Road to the Return of the State* (New York, 2023; online edn, Oxford Academic, 14 Dec. 2023).

⁴⁶ Executive Order 14110 ‘Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence’.

⁴⁷ Brazilian Ministry of Science, Technology and Innovations (2021). ‘Summary of the Brazilian Artificial Intelligence Strategy – EBIA’. Available at https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivos/inteligenciaartificial/ebia-summary_brazilian_4-979_2021.pdf (Last accessed 4 July 2024).

⁴⁸ Senado Federal, Projeto de Lei N° 2338/2023 Dispõe sobre o uso da Inteligência Artificial.

aiming to steer the development, deployment, and use of AI technologies sustainably.⁴⁹ According to the Preliminary Analysis of Bill n° 2338/2023,⁵⁰ the Brazilian DPA (Autoridade Nacional de Proteção de Dados) points out in the document, among other things, “that it is essential that the PL details issues related to the protection of personal data⁵¹ in AI sandboxes, especially in high-risk systems”. This preliminary analysis was followed by a final opinion which was published in November 2023.⁵²

Chile also took its first steps towards regulation of AI in 2023, as the Chilean Parliament began to discuss a bill on incorporating legal and ethical issues for the creation, distribution, commercialization, and use of AI.⁵³ The Bill contains 15 articles and broadly sets out, among other matters, new definitions, including a definition of AI. The Bill was developed based on Europe’s 2021 Artificial Intelligence Act and draws on an Artificial Intelligence Policy published by the Chilean Ministry of Science, Technology, Knowledge and Innovation in 2021.⁵⁴

Drawing upon previously presented documents (laws or bills), the definitions retained by each of the six selected countries were isolated and are presented in the following table (**Table 3**).

Country	Date	Document	Definition⁵⁵
Brazil	2023	Bill No. 2338 of 2023 regulating the use of Artificial Intelligence, including algorithm design and technical standards	<i>Computer system, with different degrees of autonomy, designed to infer how to achieve a given set of objectives, using approaches based on machine learning and/or logic and knowledge representation, using input data from machines or humans, with the aim of producing predictions, recommendations, or decisions that can influence the virtual or real environment.</i>
Canada	2022	Artificial Intelligence and Data Act	<i>A technological system that, autonomously or partly autonomously, processes data related to human activities through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions.</i>
Chile	2023	Proyecto De Ley Que Regula Los Sistemas De Inteligencia Artificial, La Robótica Y Las Tecnologías Conexas En Sus Distintos Ámbitos De Aplicación	<i>A software that is developed using one or more of the following techniques: a. Machine learning strategies, including supervised, unsupervised and reinforcement learning, employing a wide variety of methods, including deep learning. b. Logic and knowledge-based strategies, especially knowledge representation, inductive (logic) programming, knowledge bases, inference and deduction engines, expert and (symbolic) reasoning systems.</i>

⁴⁹ See Belli, L., Gaspar, W. B., and Curzi, Y. AI Regulation in Brazil: advancements, flows and need to learn from the data protection experience. In *Computer Law and Security Review: Special Issue on Artificial Intelligence and Data Protection in Latin America*. (2022).

⁵⁰ ANPD, Análise preliminar do Projeto de Lei n° 2338/2023, que dispõe sobre o uso da Inteligência Artificial.

⁵¹ Lei Geral de Proteção de Dados Pessoais N° 13709/2018.

⁵² ANPD, Sugestões de incidência legislativa em projetos de lei sobre a regulação da Inteligência Artificial no Brasil, com foco no PL n° 2338/2023, Nota Técnica n° 16/2023/CGTP/ANPD.

⁵³ Cámara De Diputadas Y Diputados De Chile, Proyecto De Ley Que Regula Los Sistemas De Inteligencia Artificial, La Robótica Y Las Tecnologías Conexas En Sus Distintos Ámbitos De Aplicación, 15869-19.

⁵⁴ Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, Política Nacional De Inteligencia Artificial, 2021.

⁵⁵ DeepL translator was used for bills not found in an official translated version (i.e. Brazil and Chile)

USA ⁵⁶	2023	Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence	<p><i>The term “AI system” means any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI.</i></p> <p><i>The term “artificial intelligence” or “AI” has the meaning set forth in 15 U.S.C. 9401(3): A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.</i></p>
-------------------	------	---	--

Table produced by author

⁵⁶ Regarding the USA, the Executive order is defining AI systems as ‘any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI’. However, it is possible to find a definition in the same document on AI, which includes almost all assessed criteria. Therefore, I have made the choice to go through the assessment of the USA approach.