Institut européen
European Institute

Executive Master in EU Studies

The Artificial Intelligence Act: Regulatory Competitiveness and Innovation Interference Analysis

Supervised by Prof Tamás Szigetvári

Minerva RIVERO

2025

Table of contents

Abstract

This thesis evaluates the regulatory competitiveness of the European Union in AI innovation under the EU Artificial Intelligence Act (AI Act). It first situates the Act within its stated human-rights, innovation, and digital-sovereignty justifications and analyzes its genesis and evolution through the lenses of regulatory economics and innovation theory. A legal analysis of the scope of Article 5 prohibitions shows that most restrictions are use- or actor-based rather than technology-based, rendering the framework largely technology-neutral and, in several provisions, narrow in practice. The legal analysis also reveals surprising insights into the social scoring provision. For permitted AI systems, the thesis maps the compliance architecture for high-risk AI systems, limited-risk systems, and GPAI with systemic risk, concluding that obligations are often aligned with existing technical practice. The work then assesses external factors affecting competitiveness, including the EU's legal certainty and harmonization versus U.S. regulatory fragmentation, the Regulatory Impact Assessment's trust-and-uptake channel, and EU pro-innovation initiatives such as InvestAI and the European Health Data Space. A MedTech case study demonstrates how R&D is exempt, market entry triggers high-risk controls, and post-market duties integrate into a quality-management loop. Overall, the analysis finds that the AI Act's combination of legal certainty, technology neutrality, and market-shaping reach (including the Brussels Effect) appears to position the EU to attract investment, induce both compliance and circumventive innovation, and compete effectively in AI, with implications for transatlantic firms and policymakers navigating divergent AI governance regimes.

1. Introduction

With this thesis I aim to explore the regulatory competitiveness of the EU in the AI technology innovation space in view of the AI Act by applying economic theories and exposing relevant internal and external factors. I will explore the origins and justifications of the European Union's Artificial Intelligence Act (the AI Act). Finally, I aim to illustrate the impact of the AI Act with a fictional example in the MedTech sector.

The AI Act was passed in 2024 but will not take full effect until 2 August 2026 (although a limited number of provisions entered into force in February of 2025). Thus, at present, there is no empirical data on any regulatory impact directly related to the AI Act. As such, this thesis will explore the potential regulatory compliance barriers for an innovative firm from a more theoretical and comparative perspective.

2. Justifications for the EU AI Act

On 19 February 2020, the European Commission announced the European Union's first digital strategy plan: "*Shaping Europe's Digital Future*". This communication was the genesis of the AI Act and from there we can extract at least three justifications for AI regulation: the protection of human rights, the promotion of innovation, and digital sovereignty.

2.1 Human rights protection

The Strategy communication declares:

> "An open, democratic and sustainable society: A trustworthy environment in which citizens are empowered in how they act and interact, and of the data they provide both online and offline. A European way to digital transformation which enhances our democratic values, respects our fundamental rights, and contributes to a sustainable, climate-neutral and resource-efficient economy."

Article 1 of the AI Act (titled Subject Matter) refers to:

> "ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law"

While protection of fundamental rights is one of the justifications for the AI Act, it is curious that it has received great criticism in this regard.[1]

[1] Lomas 2021.

2.2 Innovation and economy

In Section B of the communication reference is made to providing a fair and competitive economy, and to promote innovation within a framework of European values.

2.3 Digital/technology sovereignty

While not explicitly mentioned in the communication as a justification or motivation for the AI Act, we can infer, from the expressions therein in relation to the success of the General Data Protection Regulation (GDPR), that this is one of the reasons for AI regulation. Section A also emphasizes how the EU has successfully collaborated in the past in supercomputing and microelectronics.

The AI Act is thus also a geopolitical strategy that aims to make the EU relevant in the race for digital and technology sovereignty. The European Union Data Strategy and the European Health Data Space regulation are also part of this strategy and work together with the AI Act to promote digital sovereignty and innovation.

The communication justifies this geopolitical strategy on the basis of confidence derived from past successes (the *Brussels effect*):

> "The European model has proved to be an inspiration for many other partners around the world as they seek to address policy challenges, and this should be no different when it comes to digital.
>
> In geopolitical terms, the EU should leverage its regulatory power, reinforced industrial and technological capabilities, diplomatic strengths and external financial instruments to advance the European approach and shape global interactions. This includes the work done under association and trade agreements, as well as agreements reached in international bodies such as the United Nations, the OECD, ISO and the G20, with the support of EU Member States.
>
> Many countries around the world have aligned their own legislation with the EU's strong

data protection regime. Mirroring this success, the EU should actively promote its model of a safe and open global Internet."

Technology sovereignty is also discussed in the communication in the following passage:

> "It requires creating the right conditions for Europe to develop and deploy its own key capacities, thereby reducing our dependency on other parts of the globe for the most crucial technologies. European technological sovereignty is not defined against anyone else, but by focusing on the needs of Europeans and of the European social model. The EU will remain open to anyone willing to play by European rules and meet European standards, regardless of where they are based."

3. Architecture of the AI Act and Regulatory Competitiveness

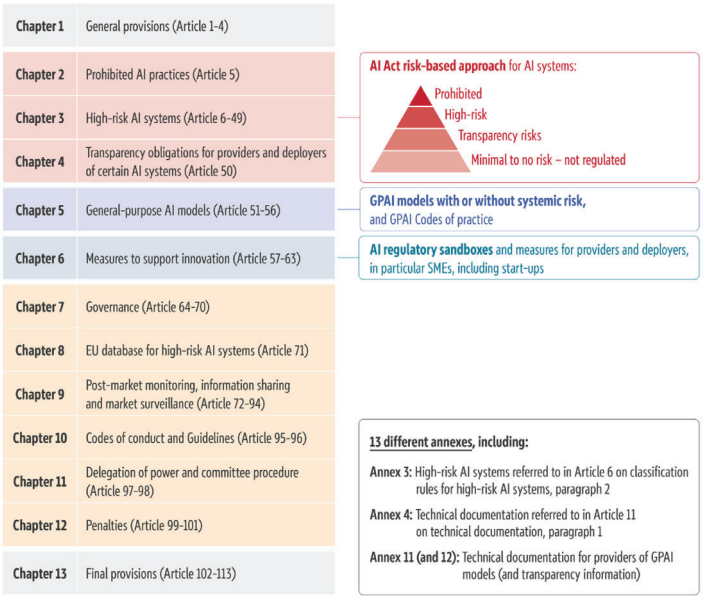

Figure 3.1 Structure of the AI Act
Image source: European Parliament AI Act Implementation timeline

The AI Act is a risk-based regulation and classifies AI systems into four risk categories: (1) unacceptable risk, (2) high-risk, (3) limited risk (not a formal label in the Act), and (4) minimal

or low-risk (not a formal label in the Act, refers to systems not subject to any of the AI Act requirements).

The restrictions in the AI Act start with a list of AI practices that are fully prohibited - AI systems with *unacceptable risk* (*Chapter II: Article 5: Prohibited AI Practices)*. Any AI system falling under the scope of Chapter II is classified as an *unacceptable risk* and cannot be practiced within the EU.

The Act then proceeds to define High-Risk AI Systems in *Chapter III: High-Risk AI System*. *Section 1 Article 6* lists the classification rules to determine whether an AI system is a *high-risk* AI system. Section 2 lists the legal requirements for high-risk AI systems.

General-purpose AI models (GPAI) are treated separately, and are not inherently part of any of the risk tiers. *Chapter V: General-Purpose AI Models* introduces classification rules for identifying General-purpose AI models and further, identifying General-purpose AI models *with systemic risk*. Providers of both classes of systems will be subject to a number of specific obligations for each class of system.

It should be emphasized that the AI Act prohibitions and all other legal compliance requirements relate only to *placing on the market or putting into service*. AI research and development is **not** affected by the Act. Article 2(6) of the Act explicitly refers to the R&D exception:

> "This Regulation does not apply to AI systems or AI models, including their output, specifically developed and put into service for the sole purpose of scientific research and development."

In summary, unacceptable risk AI systems are covered by Article 5 (the prohibitions), high risk AI systems are covered by Articles 6 and 7 with further guidelines in Annex III, limited risk AI systems are covered by transparency obligations in Article 52, minimal risk (while not explicitly mentioned and practically unregulated) are referred to in Recital 70 and implicitly mentioned

throughout the provisions, and finally, GPAI models are treated outside of the risk-based system in Article 5.

Thus, in approaching the task of evaluating the regulatory burden and innovation interference we look at it from two angles: the extent of the prohibitions, and the extent of the legal compliance burden for permitted technologies (high risk, limited risk, and GPAIs with systemic risk).

The starting point for assessing regulatory competitiveness of the AI Act is to define and interpret its actual scope. Regulations are a limitation on the freedom of action of the respectively encumbered parties. Clark Parsons, CEO of European Startup Network said: "The AI Act tried to take a light touch and only focus on risky applications. But compared to 'no touch' non-regulation in the US, light touch regulation is still regulation in the eyes of the tech community."[2] This expression gives an idea of the reception of the AI Act by the private sector.

To make an assessment of the EU's AI regulatory competitiveness we need to explore the reach of the AI Act and get a sense of its interference with AI-based innovation. For a rigorous analysis, we also need to consider external factors, such as any other relevant EU regulation and regulation in other jurisdictions. This will be explored in subsequent chapters.

In delineating the scope of the Act we can refer to *regulatory stringency - the relative degree of constraint.* As an example from another field, the OECD has published a *regulatory stringency index* for environmental regulations across the world. The general perception until now has been that the AI Act is an obstacle to innovation (as evinced by the statement above from Mr. Parsons). It has also been counter-argued that the Act is not as restrictive as it is being portrayed or perceived.[3] With the following scope analysis I hope to contribute to the understanding of the *regulatory stringency* of the AI Act.

---

[2] Greenacre 2024.

[3] *Id.*

4. Scope of the AI Act - Prohibitions

Analyzing the scope of the prohibitions can give us an idea of the extent of interference with AI innovation, which is an important factor in evaluating the regulatory competitiveness of the AI Act.

The prohibitions, also referred to as *unacceptable risk systems*, imposed by the AI Act are listed in *Chapter II: Prohibited AI practices*, specifically in Article 5(1)-(7).

I will focus on Art. 5(1) as it enumerates the restrictions on AI systems placed on the market. Art 5 (2)-(7) stipulate EU and Member State conditions/exceptions for law enforcement use of certain AI practices (which is outside the scope of this thesis). Section 8, the final section, states the non-prejudice toward AI prohibitions found in other sources of EU law in view of the AI prohibitions in the AI Act.

I will analyze each of the prohibitions (a) to (h) in turn, providing my interpretation of the scope of each prohibition and of their restrictiveness or *regulatory stringency*. Several interpretation techniques may be used to interpret legislation, such as literal, teleological or purposive, systemic, and comparative interpretation.

In this case, I will use a combination of literal interpretation enhanced with teleological and systemic interpretation derived from the recital(s) for each provision and any relevant EU legislation. A *comparative interpretation* with the US regulatory framework will be provided in the chapter discussing a MedTech case study.

But first, I will start by referring the reader to the text of Art. 5(1), reproduced below for convenience, which enumerates prohibitions (a) through (h) - corresponding to the eight separate prohibitions. I include the text here as an exercise for the reader as to the *first impression* of the scope or stringency of the provisions on the casual reader.

1. The following AI practices shall be prohibited:

(a) the placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm;

(b) the placing on the market, the putting into service or the use of an AI system that exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm;

(c) the placing on the market, the putting into service or the use of AI systems for the evaluation or classification of natural persons or groups of persons over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics, with the social score leading to either or both of the following:

(i) detrimental or unfavourable treatment of certain natural persons or groups of persons in social contexts that are unrelated to the contexts in which the data was originally generated or collected;

(ii) detrimental or unfavourable treatment of certain natural persons or groups of persons that is unjustified or disproportionate to their social behaviour or its gravity;

(d) the placing on the market, the putting into service for this specific purpose, or the use of an AI system for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics; this prohibition shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity;

(e) the placing on the market, the putting into service for this specific purpose, or the use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage;

(f) the placing on the market, the putting into service for this specific purpose, or the use of AI systems to infer emotions of a natural person **in the areas of workplace and education institutions**, except where the use of the AI system is intended to be put in place or into the market for **medical or safety reasons**;

(g) the placing on the market, the putting into service for this specific purpose, or the use of biometric categorisation systems that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation; **this prohibition does not cover any labelling or filtering of lawfully acquired biometric datasets**, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement;

(h) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless and in so far as such use is strictly necessary for one of the following objectives:

(i) the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons;

(ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack;

> (iii) the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years. Point (h) of the first subparagraph is without prejudice to Article 9 of Regulation (EU) 2016/679 for the processing of biometric data for purposes other than law enforcement.

At first glance, each provision appears rather lengthy or verbose. One can imagine that a *tech entrepreneur* or business person faced with the verbiage of these provisions might get the impression that the provisions are highly restrictive - a cumbersome obstacle to innovation and business dealing in AI-based products and services in the EU. However, a deeper and nuanced analysis might yield a different conclusion.

Additionally, some prohibitions have been denounced as too vague and difficult to detect,[4] and as such the provisions are currently very open to a wide array of interpretations. This raises the issue of legal certainty, and the final meaning of the provisions might be shaped by the subsequently developed body of case law. Each of the provisions is accompanied by references to "recitals", which offer commentary from the Union legislator on the meaning, interpretation and/or purpose of each provision.

Due to the limits of this work I will only analyze the scope of prohibitions Art. 5(1)(a), (b), (c), and (f). With the exemplary scope analyses I aim to show that, on closer analysis, the prohibitions are narrower than initial impressions suggest.

The tables below for each analyzed prohibition more readily illustrate the scope and meaning of the prohibitions. The top field of each table shows the literal text of the provision. The fields in the bottom show: the number and nature of the elements of the prohibition, a 'flipped' or version to show what *would* (theoretically) be allowed according to the provision (absent interpretation case law at this time, and subject to any other applicable Union law), and finally, an abbreviated version of the prohibition to facilitate its understanding.

[4] cf. Leiser 2024.

4.1 Art. 5 (1)(a) (Subliminal techniques)

> the placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm;

Prohibition (a)		
the placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm		
Elements required for infringement	Flipped version	Summary
(1) subliminal, purposefully manipulative, or deceptive technique (1) objective or effect (1) result, requiring a (1) specific mechanism = 4 elements	Subliminal, manipulative and deceptive techniques are allowed if: they don't cause significant harm and are not reasonably likely to cause significant harm ***by*** distorting behavior materially ***to*** impair ability to make informed decision-making*	AI techniques with the objective or the effect of distorting behaviour to impair informed decision-making such that an altered decision is taken that is likely to cause harm or actually causes significant harm.
Exception for: lawful medical and psychological therapy that does not harm. (Recital 29) *As long as otherwise legal under any other applicable Union law		

Thus, subliminal (intended to cover techniques that operate beyond a person's consciousness), and 'deceptive or purposefully manipulative' (apparently intended to cover non-subliminal techniques) are allowed as long they are not deployed with the objective, nor have the effect of, causing distortion in behavior such as to impair informed decision-making, thereby being likely to cause harm or actually causing harm.

Three main conditions are required to show infringement:

(1) an AI technique,

(2) an outcome or intended outcome (*effect or objective)* of said technique which

(3) results in *actual harm or reasonable likelihood thereof.*

A showing of infringement would not be particularly simple for this provision. It would require showing at least three conditions, which can be separated into four distinct elements, with each element further comprising a number of subelements. Generally, the more elements that must be proven to demonstrate infringement of a legal provision, the narrower its scope and the easier it is to circumvent.

Two main alternative modes of infringement are contemplated for the listed AI techniques: either having the specified objective, or having the specified effect. Both of these modes can be challenging to demonstrate. An objective of an AI technique can exist without documentation or explicit declaration thereof. It might be the case that an objective can have a detectable physical manifestation and/or be reflected in the technical implementation (in that case likely requiring a forensic investigation of the technology). But it is plausible that in many cases an infringing *objective* could be invisible to the legal eye. The *effect* mode of infringement would appear easier to prove than the *objective* mode as it would likely manifest in a physical or observable manner in the individual whose behavior is *materially distorted* thereby taking an *altered decision*.

In both cases the showing remains onerous given the degree of ambiguity and subjectivity introduced by the wording: ***materially*** distorting behavior, ***appreciably*** impairing decision-making, ***informed*** decision, decision ***that they would otherwise not have taken***, ***in a manner that causes (...)***. The bolded terms introduce *vagueness of degree.*[5] Moreover, a causal connection must be shown between each of the listed elements in the provision, which adds to

[5] cf. Poscher 2011.

the complexity of proving infringement. Thus, demonstrating infringement of the provision would be incredibly burdensome.

Provision (a) was considerably amended from the original version proposed by the European Commission in 2021. The original text was simpler:

> the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm;

The elements of *appreciably impairing their ability to make an informed decision, impairing decision-making*, and *taking a decision that they would otherwise not take*, were added during negotiations. Based on the explanation provided in the corresponding recital, we can surmise that perhaps the amendments were an attempt to prevent interference with accepted and well-known marketing techniques.

The provision also includes many terms the meaning of which we can only speculate about at this stage. What is *harm*? What is *significant* harm? What is *informed* decision-making? How can it be determined that an individual took a decision they would have otherwise not taken? Interpretation of these elements can affect the breadth of this provision (absent a definition in the Act) because their interpretation can be highly subjective. The provision is convolutedly verbose with a high degree of vagueness and ambiguity. The verbosity of the provision tends to narrow its scope, while the vagueness and ambiguity could be viewed as providing interpretative flexibility. In sum, it could be said that the provision is very narrowly drawn.

The provision is accompanied by Recital 29, which provides an indirect definition of harm: *(...) whereby significant harms, in particular having sufficiently important adverse impacts on physical, psychological health or financial interests are likely to occur (...).* This provides at least some examples of the nature of the harm that is contemplated, but remains vague on the

quantity (degree) of harm required to reach the level of *significant* harm. The lack of definition of critical terms throughout the Article 5 prohibitions are an example of semantic vagueness.[6]
Recital 29 also clarifies that:

> In addition, common and legitimate commercial practices, for example in the field of advertising, that comply with the applicable law should not, in themselves, be regarded as constituting harmful manipulative AI-enabled practices.

Additionally, *Recital 29* makes an explicit exception for medical and psychological therapies:

> The prohibitions of manipulative and exploitative practices in this Regulation should not affect lawful practices in the context of medical treatment such as psychological treatment of a mental disease or physical rehabilitation, when those practices are carried out in accordance with the applicable law and medical standards, for example explicit consent of the individuals or their legal representatives.

Technological interference

All of the Art. 5 prohibitions relate to *use-cases* and do not restrict any particular AI implementation technology itself.
As shown in Figure 4.1, the AI innovation ecosystem is comprised of five main enterprises: Chips (hardware), Foundational Models (e.g., general-purpose language models), Data (services for streaming and processing data on real-time, Generative AI (‘Gen AI’, applications generating text, audio, images etc. within a variety of contexts, such as ChatGPT), and Computing (cloud services for large computing capacity).

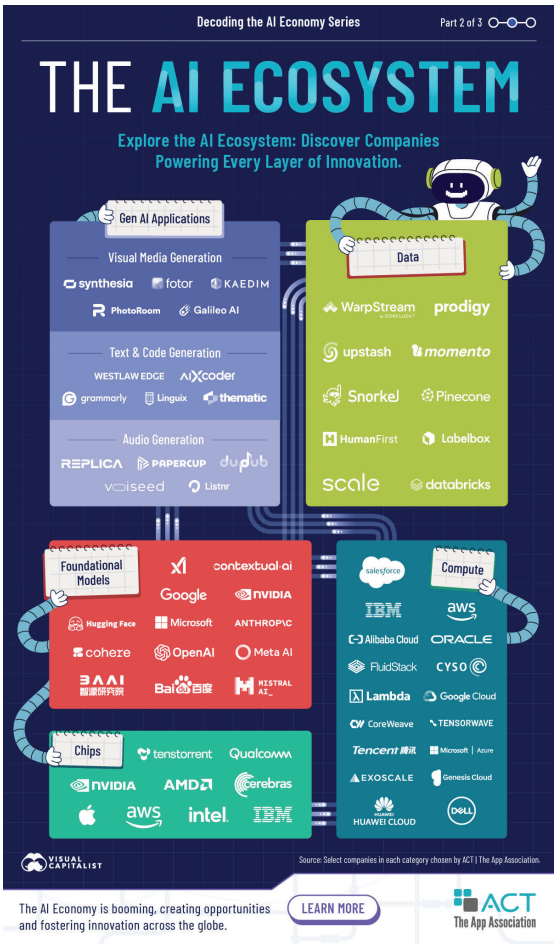

Figure 4.1 The AI Ecosystem Source: ACT The App Association

[6] cf. Poscher 2011.

The effect of prohibitions (a)-(h) would be felt in the Generative AI layer and perhaps the Data layer. Chips, foundational (general-purpose) models, computing services would generally not require adaptations (for use in developing and providing an end-user application) in a way that would be relevant for the prohibitions.

Thus, any type of AI technology (*i.e.*, 'infrastructure') can be developed to the extent that the prohibited use is not performed. It should also be noted that AI research and development (R&D) is exempt from the AI Act (*see* Art. 2(6)).

4.2 Art. 5 (1)(b) (Exploiting vulnerabilities)

> the placing on the market, the putting into service or the use of an AI system that exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm

Prohibition (b)		
the placing on the market, the putting into service or the use of an AI system that exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm		
Nature and number of elements required for infringement	Positively-recited version	Concise/summarized version
(1) vulnerability exploiting system (1) objective or effect (1) result = 3 elements	AI systems that exploit vulnerabilities of individuals are allowed if: they don't cause significant harm and are not reasonably likely to cause significant harm ***by*** materially distorting behavior Thereby causing or reasonably likely to cause significant harm to themselves or others. .	AI system that exploits vulnerabilities of individuals, with the objective or the effect of distorting behaviour in a manner that is likely to cause, or actually causes, harm to themselves or others.
Exception for: lawful medical and psychological therapy that does not harm. (Recital 29) *As long as otherwise legal under any other applicable Union law		

Thus, this is a second prohibition concerning distortion of behavior. Prohibition (b) appears to build on prohibition (a) to provide a second layer of protection for vulnerable individuals. It is broader than (a) in that it does not specifically refer to *subliminal/deceptive/manipulative techniques to distort behaviour*, rather it refers to any *material distortion of behaviour*. This provision is also accompanied by Recital 29, and thus, similar to the first provision, lawful medical treatment is exempted.

A similar infringement and term meaning analysis as for (a) would apply and will not be repeated here. A minimum of four elements will have to be shown to find infringement of prohibition (b), which is one less element than for provision (a). Moreover, the 'AI system' of prohibition (b) is much broader and easier to evince than the 'subliminal, deceptive, or purposefully manipulative AI techniques' of prohibition (a). These factors tend to show that it would be easier to prove infringement of prohibition (b) than of prohibition (a).

Recital 29 gives guidance on the meaning of vulnerabilities:

> AI systems may also otherwise exploit the vulnerabilities of a person or a specific group of persons due to their **age, disability** within the meaning of Directive (EU) 2019/882 of the European Parliament and of the Council, o**r a specific social or economic situation that is likely to make those persons more vulnerable to exploitation such as persons living in extreme poverty, ethnic or religious minorities**.

Contrast between (a) and (b)

Based on the accompanying commentary prohibitions (a) and (b) are geared towards activities like marketing and virtual reality products. Prohibition (a) is more complex, requiring more infringement elements than prohibition (b). The main distinction between provisions (a) and (b) lies in the class of citizens being protected, while (a) applies to every EU citizen, (b) is aimed at the protection of citizens with particular vulnerabilities. In this sense, (b) is narrower than (a).

Both prohibitions were present in the original EC draft of 2021. The fact that prohibition (b) had a narrower scope than (a) in the original draft (narrower class of individuals being protected) could be the reason it didn't receive much attention/pushback during the negotiation/amendment phase (e.g., pressure from private sector lobbyists).

4.3 Art. 5 (1)(c) (Social scoring)

(c) the placing on the market, the putting into service or the use of AI systems for the evaluation or classification of natural persons or groups of persons over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics, with the social score leading to either or both of the following:

(i) detrimental or unfavourable treatment of certain natural persons or groups of persons in social contexts that are unrelated to the contexts in which the data was originally generated or collected;

(ii) detrimental or unfavourable treatment of certain natural persons or groups of persons that is unjustified or disproportionate to their social behaviour or its gravity

Prohibition (c)		
the placing on the market, the putting into service or the use of AI systems for the evaluation or classification of natural persons or groups of persons over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics, with the social score leading to either or both of the following: (i) detrimental or unfavourable treatment of certain natural persons or groups of persons in social contexts that are unrelated to the contexts in which the data was originally generated or collected; (ii) detrimental or unfavourable treatment of certain natural persons or groups of persons that is unjustified or disproportionate to their social behaviour or its gravity		
Nature and number of elements required for infringement	Positively-recited version	Concise/summarized version
(1) AI system with the described purpose (1) result = 2 elements	Social scoring is allowed if: -there is no detrimental/unfavourable treatment of certain natural persons or groups of persons in social contexts unrelated to the generated/collected data - there is no detrimental/ unfavourable treatment of certain natural persons or groups of persons that is unjustified/ disproportionate to the social behaviour or its gravity	An AI system for social scoring is not allowed if it leads to unrelated, unjust, or disproportionate unfavourable treatment of even one person.

Prohibition (c)
See Recital 31

Thus,

(i) there must be a *nexus* between the social score and any detrimental/unfavorable treatment, and

(ii) any detrimental/unfavorable treatment must be justified and proportional.

Therefore, AI-based social scoring is allowed, as long as the *social score* does not lead to detrimental or unfavorable treatment of *certain* individuals in the manner defined in (i) and (ii). In this case, *certain* refers to the fact that infringing the prohibition does not require that the prohibited effects be met for all persons being evaluated/scored by the AI system.

Detrimental or unfavorable treatment of individuals on the basis of a social score is allowed as long as the social context of the score and the treatment are related, and as long as the treatment is justified and proportional. In my view, these two conditions for limiting the use of social scoring are somewhat superfluous. The first could be said to simply reflect the EU fundamental principles of fairness and non-discrimination/equality (in the sense of EU protections against treating a particular individual, arbitrarily - *without a legal justification*, differently from others), while the second relates to justice and proportionality. These are all fundamental principles in the application of EU law.

One could theorize that these fundamental principles were introduced here to bind private entities and national public authorities (when acting outside the scope of EU law) otherwise not necessarily bound by these fundamental principles. Seeing as most of the language in prohibition (c) appears to be, in my opinion, a mere reflection of fundamental principles of EU law, I don't find this prohibition (c) particularly limiting of AI innovation.

4.4 Art. 5 (1)(f) (Emotion inference)

(f) the placing on the market, the putting into service for this specific purpose, or the use of AI systems to infer emotions of a natural person **in the areas of workplace and education institutions**, except where the use of the AI system is intended to be put in place or into the market for **medical or safety reasons**;

Prohibition (f)		
the placing on the market, the putting into service for this specific purpose, or the use of AI systems to infer emotions of a natural person **in the areas of workplace and education institutions**, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons		
Elements required for infringement	Flipped version	Summary
(1) AI system with the specified objective (1) location/situation/context = 2 elements	AI systems to infer emotions of a person are allowed everywhere except in the workplace or education institutions. But, it is also allowed in workplace/education institutions if it is done for medical or safety reasons.	AI systems for inferring emotions are allowed in any space except for workplace and education institutions, but it is allowed in those places too if done for medical or safety reasons.
Exception for: medical and safety reasons *As long as otherwise legal under any other applicable Union law		

This is one of the least verbose prohibitions. It is not very restrictive as it allows the AI-based inference of emotions of people in any scenario except for the workplace and in educational institutions. Moreover, an exception is also made in said two scenarios if the emotional inference is being done for medical and safety reasons. On the other hand, the infringement burden appears easier as it requires only two main elements. Like the rest of the prohibitions it is directed at the particular *use or purpose* of the AI rather than the technology itself (it would likely only impact the application layer). It is thus not a significant prohibition in terms of interference with AI innovation.

Conclusion on scope of prohibitions of Art. 5

Most of the prohibitions are use-based or purpose-based restrictions. Some restrictions allow a particular use *but* only for certain actors. An actor-based restriction is one where the described AI system is compliant, but only if it is used by an authorised public body (the case of prohibition (h) exception for law enforcement). Another type of restriction/allowance concerns the source of the data (lawfully acquired, etc). Thus, in all cases, *technology* itself is not being restricted, rather

its use or users are (*users* in the sense of deployers, providers, distributors, and importers). In this sense, the prohibitions can be described as *technology neutral* and do not interfere much with AI technological innovation itself. As explained earlier, any interference is at the application layer of the AI ecosystem. Some of the prohibitions (e.g. (a)) are very narrowly constructed and would appear to leave plenty of room for circumvention. Thus, in my view, any effect of the Art. 5 prohibitions on AI innovation would be minimal.

5. Legal compliance burdens for permitted AI systems

5.1 High-risk AI system

Chapter III sets the rules for classifying AI-based systems as high-risk and the corresponding legal compliance requirements. The rules refer to **Annex I** and **Annex III** (Art. 6(1) and (2)), each listing conditions that automatically render a system as high risk.

Annex I is a product-triggered classification, whereby products covered by harmonised EU product safety regulations are high-risk if they comprise AI technology. For example, medical devices that include an AI component are high-risk under Annex I because medical devices per se are regulated by product safety regulation for medical devices

Annex III is a purpose/use-triggered classification, whereby an AI-based system (or the system that will have embedded AI) is classified as high-risk based on the purpose of the AI-based system.

Providers are able to **self-determine** whether their system qualifies as high-risk under Annex III (this is one of the controversial 'carve-outs' for Big Tech). Under Article 6(3) providers are allowed to derogate from Article 6(2) high risk classification, if they determine that one of the following conditions is met:

(a) the AI system is intended to perform a narrow procedural task;

(b) the AI system is intended to improve the result of a previously completed human activity;

(c) the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or
(d) the AI system is intended to perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III.

Who can be liable?

Every actor along the value/supply chain can be held liable. This is a strategy known as *extraterritoriality* and it has been identified as one of the keys in the success of EU regulation (e.g., the *Brussels effect*).

Legal requirements for high-risk systems

Providers of high-risk systems in the EU will have to comply with the requirements listed in Articles (8)-(15) in *Chapter III: Section 2: Requirements for High-Risk Systems*.

Firstly, providers must notify the notification body of its placing on the market. It should be noted that even if the result of the self-assessment is that an otherwise high-risk system falls under one of the exemptions under Art. 6(3), such a system must also be notified/registered.

These requirements are:

- establishing a risk-management system
- testing (during development or, at the latest, prior to being placed in the market or put into use)
- data and data governance requirements (such as quality of the data, and lawfully-obtained data) technical documentation
- record-keeping requirements (automatic logging of certain operation information)
- transparency
- human oversight
- accuracy, robustness and cybersecurity requirements

All providers of high-risk systems must conduct an internal conformity assessment, but only those falling under Annex I (sectoral/product-triggered classification) undergo a third-party conformity assessment by the relevant (sectoral/product) 'notified body'. While Annex III high-risk AI systems' conformity assessments need not be notified to an external body, the conformity assessment reports must be kept as part of the company records and be available for inspection. Providers of high-risk AI systems in the public services sector (or private entities providing public services) must also conduct and publish a Fundamental Rights Impact Assessment (FRIA). The FRIA must be documented and available for inspection by the relevant national supervisory authority (Art. 59 of the AI Act establishes a system of national supervisory authorities that will be coordinated by the European Artificial Intelligence Office and the European Data Protection Board where relevant. FRIA can be analogized to the Data Protection Impact Assessment (DPIA) under the GDPR.

This compliance burden will likely translate to firms needing to have at least one in-house AI regulation expert, or to contract out external AI-regulation expertise and compliance services. Moreover, the accuracy, robustness and cybersecurity requirements (referred to as the 'essential requirements') require technical knowledge. However, such requirements are unlikely to increase the compliance burden significantly as a firm designing and developing an AI system will most likely already have such technical expertise in-house, and these *essential requirements* could potentially be built-in by design into the product/system being developed.

5.2 Limited risk

While the Act does not define a 'limited risk' category, this has become the common term to refer to AI systems that do not reach the high-risk threshold, but which still pose transparency issues. Examples of these systems are chatbots/conversational AI, emotion recognition and biometric categorisation, and *deep fakes* generating systems. Providers of such systems must comply with Article 52 transparency requirements, which require that the users must be informed of the nature/actions of the system. For example, a provider of *deep fakes* must inform its users

about the falsity of what is being generated while a provider of conversational AI must inform its users that they are chatting with an AI system.

5.3 General-purpose AI models (with systemic risk)

General-purpose AI models (GPAI) with systemic risk are those GPAI models which have been deemed to pose a risk to the EU internal market, safety, health, public security, and fundamental rights in view of their capabilities. These are defined by the training computing capacity involved - exceeding 10^{25} FLOPs (floating point operations). However, systems that do not reach that threshold can still be classified as having systemic risk if it is evidenced that the system poses any of the risks mentioned earlier.

The compliance requirements for GPAI with systemic risk are: independent model evaluation and adversarial testing, reporting of any serious incidents to the European Commission, augmented cybersecurity and risk management, and documentation and access for authorities.

6. Regulatory competitiveness

To explore or study the regulatory competitiveness of the AI Act we can use different perspectives. We can look at it in macroscopic terms, such as understanding its competitiveness in the global context, or we can look at it in microscopic terms, as in predicting the behavior and decisions of businesses faced with the new AI regulations. Naturally, the macroscopic and microscopic issues do not occur in isolation and they feed into each other to a great extent.

6.1 Innovation in the economy

Since we are dealing with regulation of technology and technological innovation, we should contemplate the role of technological innovation in the economy as a point of departure for studying the economic effects of AI regulation.

Perhaps the earliest and one of the most influential scholars on the role of innovation in the economy is the Austrian economist Joseph Schumpeter (1883-1950). In his work *Capitalism,*

Socialism and Democracy, he stated (emphasis added): "The fundamental impulse that keeps the capitalist engine in motion is **new** consumers' goods, the **new** methods of production or transportation, the **new** markets, the **new** forms of industrial organization that capitalist enterprise creates."[7] Thus, per this theory the key to capitalist growth is that which is *new*, and behind that which is *new* lies *innovation*. From this tenet we can infer that more *new* translates to more growth. In *The Theory of Economic Development* Schumpeter distinguishes between an innovation phase and a subsequent phase where embodiment of the innovation actually occurs: "Theoretically we can still distinguish the carrying out of the innovation and the process of its embodiment in the circular flow as two different things."[8] Isolating these phases can be useful for policy making, and for macroeconomic and microeconomic analysis. AI technological innovation can lead (and has led) to new goods, new methods of production, and so forth. Some scholars refer to AI techniques such as machine learning as an industrial revolution of its own.[9] AI innovation has been compared to prior innovation revolutions, sometimes being referred to as the Fourth Industrial Revolution or Industry 4.0.[10] While some AI goods and services have already been placed in the market, there is still significant private and public investment going towards the R&D of AI technology. The EU, for example, recently announced the InvestAI public-private partnership to mobilize €200 billion towards AI investment. AI is expected to continue developing considerably and permeate many, if not all, aspects of life and society. When presenting *InvestAI*, Commission President Ursula von der Leyen stated: "AI will improve our healthcare, spur our research and innovation and boost our competitiveness. We want AI to be a force for good and for growth. We are doing this through our own European approach – based on openness, cooperation and excellent talent. But our approach still needs to be supercharged. This is why, together with our Member States and with our partners, we will mobilise unprecedented capital through InvestAI for European AI gigafactories. This unique public-private partnership, akin to a CERN for AI, will enable all our scientists and companies –

[7] Schumpeter 1950:83.

[8] cf. Schumpeter 1911.

[9] Makridakis 2017.

[10] Awari, El Bachour, and El Khasa 2024.

not just the biggest - to develop the most advanced very large models needed to make Europe an AI continent."[11]

Thus, applying the above Schumpeter model to AI innovation, we can characterize the state of AI in today's economy as falling mainly in the first innovation phase. At the same time, AI technology is also in an early embodiment phase. The first phase can be deemed as generating more growth, and it can give advantages to localized markets, (for example, the internal EU market) as it is more likely to provide opportunities for *appropriability* (intellectual property right monopolies) and *knowledge spillovers*.

6.2 Why regulate AI?

If, following the above economic theory, AI has significant potential for further innovation, and if innovation is an engine of economic growth, *why would the EU seek to regulate it*, thereby risking curtailing its potential and possibly hindering the EU in the global AI marketplace?

To analyze this EU regulatory action, I will apply several theories on the economics of regulation that appear to be relevant to our case. A look at these theories can also give us insights as to the regulatory competitiveness of the EU in this sector. In this work I use the term *regulatory competitiveness* to describe the effect of the AI Act in attracting or deterring innovation and capital to/from the European Union.

At the outset, we can identify a mix of public interest, capture, and institutional and political economy theories. Further, the AI Act is supplemented by incentive-based theory actions such as the AI investment fund InvestAI.

6.2.1 Public interest theory

Under the *public interest theory* regulation by the government is a needed mechanism to correct externalities such as market failures and to promote social welfare. This angle is evident in the AI Act, as it was introduced and promoted as a necessary safeguard in protecting human rights from the potential infringement by AI technology. We see reference to this objective in Article 1 of the Act, which specifies the subject matter: "The purpose of this Regulation is to improve the

[11] cf. Swinhoe 2025.

functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union and supporting innovation."

It is thus surprising that the act has received severe criticism from human rights advocates. A letter to the EU from United Nations High Commissioner for Human Rights (UNCHR) lauded the EU's initiative but expressed concern about the actual protection of fundamental rights offered by the Act. Part of the criticism stems from the concessions arguably made to "Big Tech" lobbyists during the negotiation phase of the legislation.

This segues us into the next theory: the *capture theory*.

6.2.2 Capture theory

Under the *capture theory* regulation is captured by lobbyists in service of their interests.

This process can happen gradually, with the regulated industry capturing the regulator over time through techniques such as lobbying, *revolving doors* (i.e., the bidirectional flow of individuals between employment in the private sector to employment in the public agencies that regulate their private sector), or information asymmetry (also characterized as a *principal-agent problem*).

In the case of the AI Act, Big Tech lobbyists succeeded in obtaining concessions affecting the scope of the regulation originally envisioned by the European Commission. As an example, the special chapter in the AI Act for General Purpose AI models (Chapter V) that exempts General Purpose AI models (with systemic risk) from the more stringent compliance requirements for high-risk systems was partly a result of Big Tech pressure.[12,13] This was a 'carve out' (concessions to lobbyists, whether public or private) from the original draft, which intended certain General Purpose AI models to be included in the high-risk classification of AI systems. High-risk AI systems have the most rigorous compliance requirements in the Act's risk-based

[12] cf. Perrigo 2023.

[13] cf. Vranken 2023.

framework. This exemption is also denounced in the aforementioned letter from the UNCHR (which objects to technical-based classifications (and exemptions) rather than effect(or damage)-based classifications).

An example of another concession is the derogation from Article 6 added via pars. (3) and (4) of that same article, whereby under certain (relatively broad) conditions, providers are allowed to self-assess as to whether their system are high-risk.

Considering the above examples of lobbying influence during the legislation negotiation and its outcomes, a *public interest theory* view of the AI Act might reasonably be put into question. The concessions can also provide hints as to the final scope and stringency of the Act, as generally the narrower the scope of a regulation, the less stringent it is. This would tend to support a finding that the regulation is competitive.

6.2.3 Institutional and political economy theory

Under this theory, regulation is driven by institutional and political economy objectives.
In the communications that were the genesis of the AI Act: *Coordinated Plan on Artificial Intelligence* (2018) and *Shaping Europe's Digital Future* (2020), the European Commission hints to a political strategy when it justifies regulation of digital technologies on the basis of the success of the EU's data protection strategy:

> "Many countries around the world have aligned their own legislation with the EU's strong data protection regime. Mirroring this success, the EU should actively promote its model of a safe and open global Internet. In terms of standards, our trading partners have joined the EU-led process that successfully set global standards for 5G and the Internet of Things. Europe must now lead in the adoption and standardisation process of the new generation of technology: blockchain, supercomputing, quantum technologies, algorithms and tools to allow data sharing and data usage".

The success of the EU's data strategy may be attributed both to *normative power*,[14] and to the so-called *Brussels effect.*[15] *Normative power* refers to the EU's role and perception in the global order as a force for good in setting *norms* in the promulgation and defense of fundamental rights. The *Brussels effect* is a term coined by Anu Bradford to capture the commercial standard-setting effect of EU internal regulations, which is founded on the strength of the single market and on the stringency of the standards (meeting the most stringent standard results in meeting all standards, thus causing the EU standard to be the *go-to* standard). Breaking ground with the introduction of the AI Act with the declared aim of protecting its citizens may be viewed as an example of the EU exerting its *normative power* with the expectation that its standards will be adopted across the world, or at least, by its trading partners. The EU proposal is backed by the (1) power of the single market and somewhat counterintuitively, (2) by its stringency (the Brussels effect). Thus, the AI regulatory act could also be rationalized under the *institutional and political economy theory*. Indeed, it is perceived by some observers as a geopolitical strategy.[16]

This theory can also be relevant beyond the mere initial -or *offensive*- phase of AI regulation, to describe the EU's subsequent "regulatory backsliding" in response to political pressures (private pressures were discussed under the *capture theory*, while public or political pressures are relevant under the *institutional and political economy theory)*. As a recent example, the AI Liability Directive was retreated apparently in response to foreign politician's comments at the AI Action summit.[17] This shows the *political economy* sensitivity of the EU and its balancing act in AI regulation generally.

6.3 Regulatory arbitrage: Why regulatory competitiveness matters

In this work I use the term *regulatory competitiveness* to describe the effect of the AI Act in attracting or deterring innovation and capital flows to the European Union. According to OECD

[14] cf. Manners 2002.

[15] cf. Bradford 2012.

[16] cf. Csernatoni 2025.

[17] cf. Philipponnat and Kretschmer 2025.

Working paper 15 (which discusses competitiveness in the context of *regulation impact assessments*, rather than *regulatory competitiveness* per se)[18] competitiveness is complex, multidimensional, and not easily quantifiable. As such, a mix of both qualitative and quantitative methodologies are therefore likely to be necessary. Further, innovation is identified therein as one of the three pillars of competitiveness.

The importance of regulatory competitiveness is underscored by the practice of *regulatory arbitrage,* whereby firms strategically structure their operations and/or investments to benefit from the most advantageous regulatory framework available (or combination of regulatory frameworks).[19]

Regulatory competitiveness is critical in determining a regulation's economic impact and likelihood of success. A competitive regulatory framework can be the difference between capital flight or capital attraction, and can incentivize new enterprise.[20] Reaction from both the public and private sectors (both international and domestic) to the EU AI Act shows that the mere existence of regulation can be controversial and unwelcome. Thus, the EU must exercise a careful balancing of public and private interests to ensure its regulations are competitive. Competitive regulation at the domestic level can incentivize local innovation (it has been shown that U.S. firms innovate in response to domestic regulations[21] and competitiveness at the global level can attract foreign businesses and investment.

6.3.1 Insights on Regulatory competitiveness of the AI Act

Through my research I have identified several *indicators or factors* that may provide a sense of the *regulatory competitiveness* of the EU within the AI innovation and technology space. I will

---

[18] OECD. 2021. *How Do Laws and Regulations Affect Competitiveness: The Role for Regulatory Impact Assessment*. OECD Regulatory Policy Working Papers No. 15. Paris: OECD Publishing. https://doi.org/10.1787/7c11f5d5-en.

[19] A. Riles, *Managing Regulatory Arbitrage: A Conflict of Laws Approach*, Cornell Law School Legal Studies Working Paper (Ithaca, NY: Cornell University, 2018).

[20] Knut Blind, *The Impact of Regulation on Innovation*, Nesta Working Paper No. 12/02 (London: Nesta, January 2012).

[21] cf. Blind 2012.

discuss each factor in sections **6.3.1.1-8** below. Some of these factors may be considered internal factors while others may be best described as *externalities*.

6.3.1.1 Regulatory Stringency, Scope, and Scope evolution

The metes and bounds of a regulation, or *scope*, is naturally a critical factor in determining a regulation's success. As expressed in objections from some actors in the private sector, the mere existence of regulation can be cause for antagonism *even* without regard to the actual scope of the regulation. Clark Parsons, CEO of European Startup Network stated: "The AI Act tried to take a light touch and only focus on risky applications. But compared to 'no touch' non-regulation in the US, light touch regulation is still regulation in the eyes of the tech community."[22] Therefore, it can be highly beneficial for the Union legislator to augment the public discourse with helpful, elucidating communications about the actual scope of the regulation.

Further, scope evolution (that is, amendment of the provisions throughout the legislative negotiation process) can be an indicator of the likelihood of acceptance of the AI Act by the private sector. As discussed in the previous section, several concessions or carve-outs resulted from public and private pressure, thereby rendering it narrower than originally intended and ultimately effectively reducing the obligations and actual likelihood of infringement for all potentially liable parties. These carve-outs would tend to indicate a greater acceptance of the final regulation than the one initially proposed.

Moreover, the provisions are not really *that* stringent. In many scenarios, self-assessment will suffice to meet the compliance burden, and a self-determination of *no-high-risk system* will relieve the provider from the most stringent requirements. Many AI systems (such as General Purpose AI models with non-systemic risk) fall outside the scope of most of the legal requirements.

[22] cf. Greenacre 2024.

However, stringency, in the exceptional case of the EU, appears to be a non-issue. Anu Bradford refers to the impact of stringent regulations when explaining the Brussels effect.[23] In relative terms, the EU AI Act regulation is very stringent, when compared to the near-absence of an analogous counterpart in the US, for example. But in fact, applying Bradford's findings, stringency isn't a problem, stringency is *precisely* one of the key factors of the EU's success in exporting regulations: a good/service that meets EU standards will meet the rest of the world's more lenient standards. This would tend to predict success for the AI Act.

'Necessity is the mother of invention'

Regulation can actually incentivize innovation. In the Nesta Working Paper, *The impact of regulation*, Knut Blind explains that "Circumventive innovation can be realised when the scope of the regulation is rather narrow and an innovation allows companies to escape the exposure of the regulation."[24] By contrast, "compliance innovation occurs where regulations are broad, forcing firms to innovate within regulatory constraints."[25]

In this case, we can foresee a mixture of the two: with firms operating in the high-risk AI space innovating to circumvent provisions, while firms operating outside the high-risk AI space would conduct compliance innovation.

6.3.1.2 The Brussels effect

The size of the EU market and its role as one of the world's most powerful trading blocs are a positive factor for the future success of the AI Act. Just as with the GDPR, it is predicted that the Brussels effect will be seen with at least parts of the AI Act[26]. The Union legislator strategically ensured extraterritorial applicability of the provisions in order to prevent regulatory arbitrage. Any good or service that might come into contact with the EU market will have to meet its

[23] cf. Bradford 2020.

[24] Blind 2012.

[25] *Id.*

[26] cf. Siegmann and Anderljung 2022.

conditions, even if it is not developed in the EU and even in cases where only the output itself of the AI system reaches the single market. Moreover, all actors along the supply chain are potentially liable - from providers to importers to distributors. This creates a powerful incentive for international and foreign firms to take the AI Act seriously and implement its requirements.

6.3.1.3 Provisions as market signals

As discussed in Chapter 4 concerning the scope and interpretation of some of the provisions of the AI Act, several prohibitions might be better characterized as *enablers*, rather than prohibitory rules.
In my view, such provisions may act as a signal to the market, thereby incentivizing innovation and enterprise. As an example, the AI Act is the first piece of EU legislation to mention the concept of 'social scoring'. The prohibition that might appear to the quick, unsuspecting reader to ban or prohibit social scoring - as it is part of the list of *Prohibitions* - in fact merely sets lenient limits on social scoring (its output/effect having to conform to fundamental principles of non-discrimination, fairness, and proportionality, all of which are fundamental principles of EU law).

This can be seen as a positive market signal as it lends legal certainty to the concept of 'social scoring' and its implementing AI systems, both by public and private actors.

6.3.1.4 Legal certainty

Legal certainty is an important factor which can be considered from both an internal and an externality perspective. In terms of *internal legal certainty*, the AI Act on its own can be a welcome AI innovation regulatory platform for risk-averse investors. Moreover, the EU took a EU harmonization approach towards AI regulation to ensure a level playing field throughout the Member States. This enhances legal certainty and simplifies business dealing in AI systems throughout the EU's internal market.

In terms of legal certainty viewed from an externality perspective, we can make comparisons with other jurisdictions in the global AI marketplace. Taking the United States as an example (as will be discussed in the next section) an argument can be made that the currently fragmented and *patchwork* nature of AI regulation in the US might render the harmonized EU AI regulatory framework more attractive to certain investors and innovators.

6.3.1.5 The Emerging Framework for AI regulation in the US

Federal

There is currently no binding AI regulation at the federal level. Non-binding guidance was issued by the Biden administration via Executive Order 14110 (EO14110) "*Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*."[27] However, EO14110 was revoked by the Trump administration in 2025 via Executive Order 14179 "*Removing Barriers to American Leadership in Artificial Intelligence*".

State level

The states of Colorado, Utah, California, Tennessee, Illinois, and Montana have all passed (or are in the process of passing) AI regulation to varying extents. Colorado signed its Artificial Intelligence Act into law in 2024 (focused on consumer protection). Utah signed its Artificial Intelligence Policy Act in 2024 as well, which includes legal provisions for mental health chatbots. California passed its AI Transparency Act in 2024 and currently has an AI provenance/ labeling bill pending (in the committee analysis stage). Tennessee signed the ELVIS Act into law in 2024 (focusing on protecting performers' voice and likeness from AI-generative services). Illinois enacted its AI Video Interview Act into law in 2024 and its bill on AI and Employment Discrimination becomes effective in 2026. Puerto Rico (US territory subject to federal jurisdiction) also passed several AI policy bills recently (the scope of which is limited to government use of AI).

---

[27] Executive Office of the President. 2023. "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."Federal Register 88 (210): 75191–75226. November 1.

Federal vs State

Recently, an AI moratorium blocking enforcement of any state- and city-level AI regulation was proposed as part of the "Big Beautiful Bill" (H.R.1, 119th Congress). This proposal was rejected by the Senate. Thus, state- and city-level AI regulation remains enforceable at the present time.

Voluntary

In 2023, the US National Institute of Standards and Technology (NIST) released an AI Risk Management Framework (AI RMF 1.0), consisting of voluntary guidelines AI Recommendations for anyone who designs, develops, deploys or uses AI to promote trustworthy AI systems by identifying, assessing, and managing AI risks.

US Fragmentation vs EU harmonization

As can be gleaned from the above federal and state developments, US AI regulation is in a highly uncertain state of flux. With all the developments going on, in addition to the state vs. federal conflicts, it is not accurate to describe the state of US AI regulation as a '*no-regulation'* situation (as described by some actors in the private sector).

Thus, there is at present a stark contrast between the harmonized EU regulatory framework and the highly fragmented and uncertain AI regulatory situation of the United States.

6.3.1.6 Regulatory Impact Assessment

The Regulatory Impact Assessment (RIA) of 2021 by the European Commission discusses competitiveness in relation to different AI regulatory policy options. It contemplates factors such as compliance costs and public trust and uptake of AI for each of the options. In relation to Option 3 (which is the risk-based, sector-agnostic (horizontal) AI policy that was ultimately selected), the report states that the risk-based system - which imposes strict requirements on

high-risk systems - would increase public trust, and therefore, uptake of AI goods and services (a positive for competitiveness). Thus, per the report, public trust and uptake is another indicator of the success and regulatory competitiveness of the regulation, as it is hypothesized that such trust and uptake, emanating from the regulation, would increase demand for AI goods and services. In the Commission's envisioned model, risk-based obligations and transparency increase trust, and trust, in turn, increases uptake. This constitutes a "trust-and-uptake channel" that can offset compliance frictions and support competitiveness. However, the assessment also states that it would increase compliance costs for *high-risk* AI systems, which in turn might deter innovation in the high-risk AI system space within the EU, with firms preferring to innovate in the lower-risk AI space.

6.3.1.7 InvestAI

Some positive externalities that I have identified are the recently announced EU InvestAI investment fund, which is a public-private partnership effort that has pledged €200 billion to fund AI innovation (such type of initiative would fall under the *incentive theory* of economics of regulation). This initiative should help to subsidize, either directly or indirectly, the compliance costs of AI firms. It also includes AI innovation assistance specifically targeted at SMEs.

6.3.1.8 Data Strategy

Another positive externality is the recently enacted European Health Data Space (EHDS) regulation. This regulation has the potential to produce one of the largest collections (if not the largest) of health data worldwide. The definition of *health data* under this regulation is impressively broad, including not only traditional health (medical) data, but also behavioral, genetic data, social and education factors. This can be a valuable opportunity for AI providers, especially in the MedTech space, as it can offer a powerful dataset for training AI models.

7. MedTech case study

To illustrate the regulatory impact on an AI-based business we will look at a fictional MedTech company: a small enterprise currently developing an online-based, remote mental health psychological therapy service.

For each therapy session, the therapy will be AI-generated based on combination of direct verbal user input and biometric-based emotion recognition. Some of the biometric parameters they plan to use are voice characteristics (tone, pitch, volume), and facial expressions (facial/visual cue emotion recognition). The system will further store collected data and use it to improve the service for further sessions with that user/patient (and maybe to improve the overall service).

So, what regulatory hurdles will a MedTech start-up encounter when choosing to innovate and place their product in the EU market?

For purposes of this analysis, I will simplify the business stages to the following: R&D, placing on the market, and post-market.

7.1 Research & Development

According to Art. 2(5) of the Act:

> The AI Act **does not apply** to AI systems and models specifically developed and put into service **for the sole purpose of scientific research and development**.

Thus, the R&D phase of AI-based systems is not directly affected by the AI Act, as the prohibitions and legal compliance requirements are limited only to AI-based systems that are actually placed in the market (or put into use, such as by governments).

Thus, in this phase MedTech will have broad freedom to act (subject to any compliance requirements outside of the AI Act), for as long as their system is not yet placed in the market. This provides room or a flexibly regulatory space for experimenting (e.g. iterations of developing, testing, and evaluating prototypes) with their AI solutions, without the fear of fines or lawsuits under the AI Act. This allows MedTech to explore design or options and select the best prototype prior to market launch.

In fact, the EU AI strategy offers opportunities for this business phase. InvestAI, a €200 billion private-public partnership investment aims to provide funding for research start-ups and to build 13 AI gigafactories.

EC President Ursula von der Leyen stated:
"AI will improve our healthcare, spur our research and innovation and boost our competitiveness. We want AI to be a force for good and for growth. We are doing this through our own European approach – based on openness, cooperation and excellent talent. But our approach still needs to be supercharged. This is why, together with our Member States and with our partners, we will mobilise unprecedented capital through InvestAI for European AI gigafactories. This unique public-private partnership, akin to a CERN for AI, will enable all our scientists and companies – not just the biggest - to develop the most advanced very large models needed to make Europe an AI continent."[28]

Regulatory sandboxes

The AI Act provides for the creation of regulatory sandboxes, but these are left to the Member States. These offer an opportunity for enterprises to experiment within the ethical boundaries of the EU. Our fictional MedTech firm may make use of regulatory sandboxes depending on the Member State where the business is domiciled. It is predicted that Member States may stipulate conditions for selecting firms that may make use of their regulatory sandboxes. A firm choosing

[28] cf. Swinhoe 2025.

to use a regulatory sandbox should take measures to avoid exposing their intellectual property and trade secrets.

7.2 Placing on the market

A firm providing a product or service according to the example case would fall under the general scope of the AI Act, per Art. 2(a) as a *provider placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the Union, irrespective of whether those providers are established or located within the Union or in a third country.*

Thus, the firm must ensure its system and its operations comply with the applicable AI Act requirements.

First step - check whether any of the mechanisms of operation of the product falls under Chapter II: Article 5: Prohibited Practices

As a first step (and ideally prior to development) the firm should check whether the provided product falls under one of the prohibitions of Article 5. In particular, Article 5(a) and (b) would be relevant for the example case. These two provisions relate to AI systems which *materially distort behavior* (provision (a) is a general prohibition while provision (b) focuses on systems that exploit vulnerabilities of a user such as age or disability). A challenger to the example product could perhaps argue that AI-based psychological therapy might, in some cases, *materially distort behavior.* However, if the distortion does not impair informed decision-making, and further, if it is not likely to cause harm, and in fact, does not result in harm (of the user or others), then such a product would not be prohibited under Article 5. Psychological therapy aims to positively benefit (or heal) the user or patient, as such, it would likely be difficult that such a provider intends to cause harm or that such service would likely cause harm. Moreover, *Recital 29* accompanying these two provisions, clarifies that:

"The prohibitions of manipulative and exploitative practices in this Regulation should not affect lawful practices in the context of medical treatment such as psychological treatment of a mental disease or physical rehabilitation, when those practices are carried out in accordance with the applicable law and medical standards, for example explicit consent of the individuals or their legal representatives."

Thus, the example product (providing psychological treatment as mentioned in Recital 29) would most likely not be subject to the provisions of Article 5, as long as any *manipulative or exploitative* practices (with the objective of psychological treatment) are carried out in compliance with other applicable law, medical standards, and consent of the user/patient.

Second step - check if it is a high-risk system under Chapter III: High-Risk Systems

Now that the provider is aware that they are not conducting any prohibited practices (or that such practices are exempted from Article 5 due to providing medical/psychological treatment), the provider should look into whether their AI-based system is a *high-risk system* per the AI Act.

To do so, the provider should look at Article 6 of Chapter III, which stipulates the rules for classifying AI-based systems as *high risk*.

The classification rules make reference to Annex I (Art. 6(1) and Annex III (Art. 6(2), contain lists of provisions that automatically render a system as high risk. Annex I relates to products covered by harmonised EU product safety regulations, while Annex III concerns high risk identification based on sectors, or based on the purpose/specific use of the AI-based system (or the system that will have embedded AI). Annex III relates to AI-technique specific risks.

Our example product likely falls within the scope of both annexes.

Firstly, it is likely covered as a medical device by item 11 of Annex I: 11. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1). A medical product would be covered by (c) emotion recognition.

Secondly, as our example product would use biometrics for emotion recognition for tailoring psychological therapy, it would be captured as an AI system using biometrics by Annex III under item 1(c) *AI systems intended to be used for emotion recognition*.

It should be noted that providers are able to self-determine whether their system classifies as high-risk under Annex III. Under Article 6(3) providers are allowed to derogate from Article 6(2) high risk classification, if they determine that one of the following conditions are met:

> (a) the AI system is intended to perform a narrow procedural task;
> (b) the AI system is intended to improve the result of a previously completed human activity;
> (c) the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or
> (d) the AI system is intended to perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III.

Our example case would likely not fall under any of these exemptions. More specifically, it would likely not fall under any of the exemptions as follows: (a) the ultimately delivered psychological therapy is not a procedural task but more of an output/final outcome of the system, (b) the system would not improve a previously completed human activity (unless the product is used only to enhance therapy provided by a (human) psychologist, (c) the product would adapt or tailor each session to the particular patient (and adapt each session for a patient) and thus would not be merely detecting decision-making patterns and replacing or repeating such, and finally (d)

the product would not be limited to performing a preparatory task but would provide an outward-facing output beyond mere internal preparation.

Thus, we can conclude that our MedTech product example would most likely classify as a high-risk AI-based system, both under Article 6(1) (Annex I) and under Article 6(2) (Annex III).

Now that we have determined that the product is high-risk, what requirements must it comply with?

As a provider of a high-risk system in the EU our MedTech example will have to comply (*see Chapter III:Section 3: Obligation for Providers of High-Risk Systems*) with the requirements listed in Articles (8)-(15) in *Chapter III: Section 2: Requirements for High-Risk Systems*.

Firstly, it has to notify the notification body of its placing on the market. It should be noted that even if the result of the self-assessment is that an otherwise high-risk system falls under one of the exemptions under Art. 6(3) such a system must also be notified/registered.

These requirements include establishing a risk-management system, testing (during development or, at the latest, prior to being placed in the market or put into use), data and data governance requirements (such as quality of the data, and lawfully-obtained data), technical documentation, and record-keeping requirements (automatic logging of certain operation information), transparency, human oversight, and accuracy, robustness and cybersecurity.

Thus, considerable internal systems will have to be developed in-house or procured in order to meet the requirements.

7.3 Post-market compliance

Our mental health AI start-up will have to comply with monitoring and documentation requirements post-market that would be part of the firm's Quality Management System (QMS) mandated by the AI Act. It must also provide human oversight of the compliance requirements. It must collect real-world performance, complaints, near-misses, and monitor the *essential requirements* of accuracy, robustness, and cybersecurity. It must keep automatic logs and technical documentation up to date. It must report any serious incidents and malfunctions without undue delay to the AI national authority (and the sectoral notified body - in this case, an MDR notified body). It must also implement corrective and preventive actions such as patches, model updates and field notices/recalls.
If the firm's model is substantially modified then a new conformity assessment must be conducted. It must also comply with the MDR post-market surveillance requirements.

7.4 Opportunities for MedTech

7.4.1 European Health Data Space

The European Health Data Space (EHDS) regulation will likely create one of the largest (if not the largest) databases of homogenized health data in the world. Moreover the definition of what data qualifies as health data is incredibly broad. Data is one of the engines of some AI systems, and access to such a large database can provide business opportunities for firms, especially in the MedTech and HealthTech sectors.
For the surprisingly broad meaning and scope of 'health data', see paragraph (6) of the European Union Health Data Space regulation (single market of data):

> "More and more individuals living in the Union cross national borders to work, study, visit relatives, or for other reasons. To facilitate the exchange of health data, and in line with the need to empower citizens, they should be able to access their health data in an electronic format that can be recognised and accepted across the Union. Such personal electronic health data could include personal data related to the physical or mental health of a natural person, including related

> to the provision of healthcare services, and which reveal information about that natural person's health status, personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question, as well as data determinants of health, such as behaviour, environmental and physical influences, medical care, and social or educational factors. Electronic health data also include data that have been initially collected for research, statistical, health threat assessment, policymaking or regulatory purposes and it should be possible to make them available in accordance with the rules laid down in this Regulation. Electronic health data consist of all categories of those data, irrespective of whether such data are provided by the data subject or other natural or legal persons, such as health professionals, or are processed in relation to a natural person's health or well-being and should also include inferred and derived data, such as diagnostics, tests and medical examinations, as well as data observed and recorded by automated means."

Thus, the scope of health data includes typical medical data but also behavioral, genetic data, social and education factors all under the umbrella category of 'health data'.

7.4.2 InvestAI

The InvestAI initiative will provide access to funding and AI gigafactories, with a special focus on small and microenterprises (SMEs). This is thus another opportunity for firms in the MedTech sector, and especially for new entrants.

7.5 How does it compare to US compliance?

In the US our example product would have to meet FDA regulations, including the Software as a Medical Device regulation (SaMD).

A software-based medical device would fall under the scope of SaMD (21 U.S.C. § 321(h)) if (1) it is intended for medical use, (2) concerns software that functions independently of a physical medical device, (3) the software informs or guides clinical decisions (especially those

that impact treatment or diagnosis, and (4) it meets certain risk classification level based on the severity of the medical condition or the degree of impact of treatment and it is not exempted under the low-risk wellness ‘app’ exception.

Thus, it is very likely our example product would be covered. A requirement is that the provider must submit a pre-market notification. This involves a submission fee of approximately 22000 USD. In contrast, no such fee has (until now) been announced in the EU for the high-risk system notification requirement.

Moreover, our example provider would have to deal with state-level regulation. Some states have adopted AI-regulation that would likely be relevant for an AI-based psychological therapy provider such as: California, Colorado, Utah, and Montana.

While the EU’s pioneering AI regulation might be seen by some as an interference with innovation, it at least provides a uniform level of legal certainty. A provider operating in the US will have to comply with different AI requirements in different states (or perhaps avoid marketing their product in those states). In this sense, the EU offers more legal certainty than the United States. Studies have shown that a benefit of legal certainty is that it can increase investor trust, and this can be critical for SMEs.[29]

On the other hand, compliance with EU regulations could be costly. The 2021 AI RIA report recognizes the compliance burden and admits that smaller businesses are less likely to be able to afford it. However, the EU appears to address these issues by providing certain accommodations for SMEs (such as simplified documentation and access to AI gigafactories).

[29] cf. Hutahayan, Fadli, Amimaknur, and Dewantara 2024.

8. Conclusions

I began this research with the initial assumption that the AI Act posed stringent regulation that might hinder innovation in the EU and disfavor investment towards AI in the coming years. However, my research has led me to conclude that the AI Act is poised for success: it provides legal certainty where other markets are rocking back and forth in a sea of uncertainty and internal conflict. This is particularly relevant when compared to the multidimensional fragmentation (sectoral, state/city) of AI regulation development in the US. Investors, businesses, and entrepreneurs tend to value legal certainty.

Moreover, the stringency of the regulation is not particularly high and it does not appear to materially interfere with actual technological development. Restrictions and prohibitions relate to the *use or purpose* of AI systems, rather than their technological implementation. That is, the AI Act is mostly technology-neutral. In that sense, it does not pose a barrier to technological innovation, as compliant uses and applications can surely be found for innovative AI-technology (this has been termed by some economists as '*compliance innovation*'). In the alternative, firms can practice 'circumventing innovation' and find new, creative ways to approach problems and solutions that do not trigger the AI Act provisions (or at the very least, avoid the most burdensome obligations). Thus, regulation *can* be a source of innovation.

Moreover, the scope of some provisions is such that they could be characterized as *enabler* or *platform* provisions that can signal to the market that national (or EU) governments might be open to procuring new goods and services (such as social scoring systems) - this is an opportunity for new research & development and product offerings by AI firms.

Additionally, the European Union Data Strategy as well as the InvestAI initiative bolsters the possibilities, in particular with the new EHDS regulation: a great opportunity for firms in the MedTech and HealthTech spaces.

All of these factors, coupled with the well-known *Brussels effect* lead me to conclude that the AI Act lends the EU with high regulatory competitiveness in the AI sector, and that it will likely succeed in promoting innovation and attracting AI investment.

Bibliography

Almada, Marco (2024). The Brussels side-effect: On the power of EU information law outside the EU. *German Law Journal, 25*(7), 1459–1481. https://doi.org/10.1017/glj.2024.83.

Arrow, Kenneth J. (1963). Uncertainty and the welfare economics of medical care. *American Economic Review, 53*(5), 941–973. https://doi.org/10.2307/1812044.

Blind, Knut (2012). *The Impact of Regulation on Innovation.* Nesta Working Paper 12/02. London: Nesta.

Borisoglebskaya, Alina (2025, Mar. 14). Europe's AI bet: Does it have what it takes to deliver? *EUobserver*. https://euobserver.com/opinion/160123.

Bradford, Anu (2012). The Brussels Effect. *Northwestern University Law Review, 107*(1), 1–68. https://www.law.northwestern.edu/lawreview/v107/n1/1/LR107n1Bradford.pdf.

Bradford, Anu (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.

California State Legislature (2024). *California AI Transparency Act*, SB 942, 2023–2024 Reg. Sess., ch. 291 (codified at Cal. Bus. & Prof. Code § 22757 et seq.; operative Jan. 1, 2026).

Carnegie Endowment for International Peace (Clark, Mason) (2025, June 12). Europe's AI power play: Can InvestAI match U.S. and China? https://carnegieendowment.org/2025/06/12/europes-ai-power-play-can-investai-match-us-and-china-pub-123456.

Colorado General Assembly (2024). *Consumer Protections for Artificial Intelligence*, SB24-205, ch. 198 (signed May 17, 2024; key duties effective Feb. 1, 2026).

Council of Europe (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (opened for signature May 2024). https://www.coe.int/en/web/artificial-intelligence/fcai.

Csernatoni, Raluca (2025, May 20). *The EU's AI Power Play: Between Deregulation and Innovation.* Carnegie Endowment for International Peace — Carnegie Europe. https://carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation?lang=en.

DatacenterDynamics (2025, Feb. 11). EU to invest €20bn in four 'AI gigafactories'. https://www.datacenterdynamics.com/en/news/eu-to-invest-20bn-in-four-ai-gigafactories/.

Den Hertog, Johan (2007). A review of economic theories of regulation. *TILEC Discussion Paper*, DP 2007-030. https://pure.uvt.nl/ws/portalfiles/portal/1142046/2007-030.pdf.

EASA (EU Aviation Safety Agency) (2024). Regulation (EU) 2024/1689 – Official Journal reference page. https://www.easa.europa.eu/en/document-library/regulations/regulation-eu-20241689-european-parliament-and-council.

EU Council (2024). Decision (EU) 2024/2218 on signing the Council of Europe AI Convention. https://eur-lex.europa.eu/eli/dec/2024/2218/oj/eng].

European Commission (2020). *A European Strategy for Data* (COM(2020) 66 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066.

European Commission (2021). *Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act)* (COM(2021) 206 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

European Commission (2025, Feb. 10–11). EU launches InvestAI initiative to mobilise €200 billion for AI, incl. €20bn fund for AI gigafactories (Press release IP/25/467). https://ec.europa.eu/commission/presscorner/detail/en/ip_25_467.

European Commission (2024). AI innovation package (Jan. 2024) backgrounder. https://digital-strategy.ec.europa.eu/en/factpages/ai-innovation-package.

European Commission (2025). Apply AI initiative announcement (Apr. 2025). https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14625-Apply-AI-Strategy-strengthening-the-AI-continent_en.

European Parliament Research Service (2025). *Artificial intelligence: Key issues at a glance* (At a Glance, PE 772.906). https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2025)772906.

European Union; European Parliament and Council (2024). Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union, L* (2024/1689), 12 July 2024. http://data.europa.eu/eli/reg/2024/1689/oj.

European Union; European Parliament and Council (2024). Regulation (EU) 2024/1261 establishing a European Health Data Space. *Official Journal of the European Union, L 119*, 8 May 2024, 1–130. http://data.europa.eu/eli/reg/2024/1261/oj.

Executive Office of the President (Biden) (2023, Oct. 30). Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

Executive Office of the President (Trump) (2025, Jan. 20). Executive Order 14148: Initial Rescissions of Harmful Executive Orders and Actions. https://www.federalregister.gov/documents/2025/01/23/2025-01531/initial-rescissions-of-harmful-executive-orders-and-actions.

Executive Office of the President (Trump) (2025, Jan. 23). Executive Order 14179: Removing Barriers to American Leadership in Artificial Intelligence. https://www.federalregister.gov/documents/2025/01/28/2025-01792/removing-barriers-to-american-leadership-in-artificial-intelligence.

Food and Drug Administration (2019, Apr. 2). *Proposed Regulatory Framework for Modifications to AI/ML-Based Software as a Medical Device (SaMD): Discussion Paper and Request for Feedback*. https://www.fda.gov/media/122535/download.

Food and Drug Administration (2021, Jan. 12). *AI/ML-Based Software as a Medical Device (SaMD) Action Plan*. https://www.fda.gov/media/145022/download.

Food and Drug Administration (2025, Mar. 25). Artificial Intelligence and Machine Learning in Software as a Medical Device (SaMD). https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device.

GovAI (Siegmann, Janis) (2022). *The Brussels Effect and AI Governance* (Brief). https://www.governance.ai/research/the-brussels-effect-and-ai-governance.

GovAI (Siegmann, Janis; Anderljung, Markus) (2022). *The Brussels Effect & AI governance*. Centre for the Governance of AI. https://www.governance.ai/research/the-brussels-effect-and-ai-governance.

Interface Europe (Debate transcript) (2024). Policy debate transcript on the EU AI Act 'gigafactories' initiative. https://www.europarl.europa.eu/doceo/document/CRE-9-2024-03-12-ITM-012_EN.html.

International Association of Privacy Professionals (IAPP) (2025). Neurotechnologies under the EU AI Act: Where law meets science. https://iapp.org/news/a/neurotechnologies-under-the-eu-ai-act-where-law-meets-science/.

Laffont, Jean-Jacques, & Tirole, Jean (1991). The politics of government decision-making: A theory of regulatory capture. *Quarterly Journal of Economics, 106*(4), 1089–1127. https://doi.org/10.2307/2937958.

Manners, Ian (2002). Normative power Europe: A contradiction in terms? *Journal of Common Market Studies, 40*(2), 235–258. https://doi.org/10.1111/1468-5965.00353.

Montana Legislature (2025). *Right to Compute Act*, SB 212 (signed Apr. 16, 2025).

Montana Legislature (2025). *Limit government use of AI systems*, HB 178 (signed May 5, 2025; effective Oct. 1, 2025).

OECD Regulatory Policy Working Papers, No. 15

Davidson, Kauffmann, and de Liedekerke (2021). *How Do Laws and Regulations Affect Competitiveness: The Role for Regulatory Impact Assessment.* OECD Publishing.

OECD (2019). *OECD Principles on Artificial Intelligence*. https://oecd.ai/en/ai-principles.

Peltzman, Sam (1976). Toward a more general theory of regulation. *Journal of Law and Economics, 19*(2), 211–240. https://doi.org/10.1086/466865.

Posner, Richard A. (1974). Theories of economic regulation. *Bell Journal of Economics and Management Science, 5*(2), 335–358. https://doi.org/10.2307/3003113.

Puerto Rico Senado (2025). *Proyecto del Senado 68 (P. del S. 68)*: Para establecer la política pública en materia de inteligencia artificial (presented Jan. 2, 2025).

Hutahayan et al. (2024). Investment decision & legal certainty under the EU AI Act. *Cogent Business & Management*. Volume 11, Issue 1. https://doi.org/10.1080/23311975.2024.2332950.

Reuters (2024, Sept. 18). Cruz, House Republicans oppose EU's plan to build AI-assisted computer network. https://www.reuters.com/world/us/cruz-house-republicans-oppose-eus-plan-build-ai-assisted-computer-network-2024-09-18/.

Riles, Annelise "Managing Regulatory Arbitrage: A Conflict of Laws Approach." *Cornell International Law Journal.* Cornell Law School Legal Studies Working Paper (2018).

Science|Business (2025). EU is 'losing the narrative battle' on AI. https://sciencebusiness.net/news/ai/eu-losing-narrative-battle-over-ai-act-says-un-adviser.

Sonková, Magdaléna (2024). The EU's quest for digital sovereignty: Policy, geopolitics, and power. *College of Europe Policy Brief (CEPOB)*, No. 3/2024. https://cadmus.eui.eu/handle/1814/76850.

Stigler, George J. (1971). The theory of economic regulation. *Bell Journal of Economics and Management Science, 2*(1), 3–21. https://doi.org/10.2307/3003160.

Tennessee General Assembly (2024). *Ensuring Likeness, Voice, and Image Security (ELVIS) Act*, HB 2091 / SB 2096 (signed Mar. 21, 2024; effective July 1, 2024).

Utah Legislature (2024). *Artificial Intelligence Amendments (Artificial Intelligence Policy Act)*, SB 149 (signed Mar. 13, 2024).

Visual Capitalist (2025, June 7). *AI Ecosystem: An In-Depth Guide.* Visual Capitalist. https://www.visualcapitalist.com/sp/taa02-ai-ecosystem/.

Vogel, David (1995). *Trading Up: Consumer and Environmental Regulation in a Global Economy*. Harvard University Press.

Vogel, David (1997). Trading up and governing across. *Journal of European Public Policy, 4*(3), 556–571. https://doi.org/10.1080/13501769780000051.