A COMPARATIVE ANALYSIS OF ARTIFICIAL INTELLIGENCE IN THE UNITED STATES OF AMERICA AND THE EUROPEAN UNION

Bálint Vitkovics*

1. Introduction

Spectacular technological developments of recent years, and the emergence of artificial intelligence (AI) in particular have fundamentally changed the way we see individuals, society, and their relationship with each other. For years, experts in jurisprudence have asked the question: is it time to regulate this new technology by law? The answer goes beyond mere legal technicalities, as it raises serious ethical questions, which also implies a serious choice of values about how we see the future of regions, countries, and of course, the individual and humanity itself.

It is therefore no coincidence that the legal professionals of the two dominant economic and cultural blocs in the Western hemisphere, the United States of America (US) and the European Union (EU) have recently engaged in a serious debate on the need for regulation of AI. In this paper, we attempt to compare the legislative approaches taken so far by the US and the EU, including what they emphasise, how they assess the intensity of regulation, and precisely what they intend to regulate and how.

* PhD student, Eötvös Loránd University (ELTE).

2. Do we really need to regulate technology?

The regulation of technology has a relatively long history.[1] One of the most important dilemmas of this process is how far the regulation that is being introduced will hinder the potential dynamics of technological development. In the literature on regulation, it has also been argued that legislation itself can be described as a kind of technology, whereby the legislator chooses between available instruments, so regulation is only an *instrument choice*.[2] We cannot agree with this position, as although legislation is always a choice between soft or hard law instruments, but the very basis for this is a value choice, and this *choice of values* can determine the instruments themselves.

The first step in an appropriate legislative intervention is based on the assessment of the situation and the extent to which legislation is needed.[3] From a logical point of view, this analysis can lead to two possible outcomes: either the existing legislation is able to deal with the change, even if the change challenges it to some extent, or we are experiencing a significant change, the main characteristics of which were unknown to the legal system before, thus finding new solutions and making new legislation are justified.[4] Practically, this analysis is a kind of legislative risk assessment, which identifies the main problems, their possible consequences and, on this basis, the regulatory concept.

A further challenge in regulating technology is that even if the legislator concludes based on the risk assessment that some level of intervention is warranted, we do not have all the necessary knowledge when the need for regulation arises, which brings us back to the original question: do we really need to regulate technology at this point?[5] This uncertainty and doubt that accompany regulation can give people the impression that law is always chasing after events. We can break out of this vicious circle by drawing on the knowledge we have accumulated so far, by taking a close look at both good and bad experiences.

---

1 Jonathan B. Wiener: The regulation of technology, and the technology of regulation. *Technology in Society,* 2–3/2004. 483–484. DOI: 10.1016/j.techsoc.2004.01.033

2 Ibid. 484.

3 See Tóth, András: *A technológia szabályozásának jogi kihívásai*. In. Tóth András (ed.): *Technológia jog – Új globális technológiák jogi kihívásai*. Budapest, KRE ÁJK, 2016. 27.

4 Klein, Tamás – Tóth, András (ed.): *Technológia jog – Robotjog – Cyberjog.* Budapest, Wolters Kluwer, 2018. https://uj.jogtar.hu/#doc/db/195/id/A18Y1766.YOV/ts/10000101/lr/chain903

5 See Antonio D'Aloia: Il diritto verso „il mondo nuovo". Le sfide dell'Intelligenza Artificiale. *BioLaw Journal – Rivista di BioDiritto,* 1/2019. 12–14.
DOI: https://doi.org/10.15168/2284-4503-349

It is difficult to talk about successes and failures of regulation in a summarised way, because of the great diversity of solutions in practice, such as the different methods in impact assessments or regulatory-deregulatory approaches.[6]

In this paper, we are putting this idea into practice and we examine the findings of US and European legislators related to the increasing use of artificial intelligence (AI) with the emphasis set on how they translated their observations into the language of law.

3. Common background

The history of AI dates back to the 1950's. In that decade, British-born Alan Turing published his fundamental article in the academic journal called *Mind* on AI. In 1956, in Dartmouth College, New Hampshire, the first ever workshop on AI was held. Over the past decades, a lot of research was carried out and academic literature was written on this subject, but until recently, legislation has not really addressed AI on a comprehensive level. This is not to say, of course, that there are no references to AI in US and European legislation at all, but it has only emerged as a separate legal subject to be regulated in recent years.

For both the USA and the EU, 2018 is the year to highlight, as this is when AI regulation got a major boost in both blocs. In the case of the EU, the European Commission (EC) issued its communication[7] setting the EU's first holistic AI strategy in motion. In addition, a high-level expert group on AI (called HLEG) 52 experts was set up to provide technical input for the EC. In 2019, the EC set out to strengthen the digital single market[8] with a number of initiatives

[6] See Wim Voermans: To measure is to know: the quantification of regulation. *Theory and Practice of Legislation,* 1/2015., DOI:10.1080/20508840.2015.1041706.91; Helen Stout – Martin de Jong: Exploring the impact of government regulation on technological transition. A historical perspective on innovation in the Dutch network-based industries. *Laws,* Vol. 9., N. 1. (2020) DOI: 10.3390/laws9020011; Lucy Firth – David Mellor: The impact of regulation on innovation. *European Journal of Law and Economics,* 3/1999.

[7] European Commission COM(2018) 795 final, Coordinated Plan on Artificial Intelligence (hereinafter: Communication I) and European Commission COM(2018) 237 final, Artificial Intelligence for Europe (hereinafter: Communication II)

[8] The EC sees the Digital Single Market as part of the Single Market, of which AI itself is a segment too. This train of thought is legally relevant. Under Article 3(1)(b) of the Treaty on the Functioning of the European Union, the EU has exclusive competence to establish the competition rules necessary for the functioning of the internal market, while under Article 4(2)(a) EU has shared competence with the Member States for the internal market as a whole. This gives the EU a wide margin to manoeuvre, based on which the EC can propose EU legislation.

resulting in EU legislation,[9] including the publication of the EC's White Paper and the European Data Strategy in 2020. In 2021, the EC revised its AI Strategy and issued a proposal for a Regulation for the use of AI-based tools with a general approach. The proposal was supported at first reading by the European Parliament, but its text had more than 700 proposed amendments in 2023.

In the US, the White House hosted a summit called "AI for American Industry" in 2018. As a result, the President of the US issued Executive Order 13859 on 11 February 2019. In 2020, a memorandum linked with this executive order was published by the White House's Office of Management and Budget (OMB) which included principles for future regulation on AI. Also worthy of note is the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, which included the AI Initiative Act of 2020 (AI Initiative Act). Executive Order 13960 and the AI in Government Act were also issued in 2020. Finally, a major milestone was the publication of the Blueprint for an AI Bill of Rights (Blueprint) in October 2022.

At the 2018 summit held in the US, invited experts sought answers to the question of maintaining US leadership in AI research and development.[10] This is very much in line with the European approach, which is also essentially economy-focused and wants to ensure EU leadership in AI development.[11] In this respect, the two major blocs are on the same page: they see AI as a huge opportunity primarily from an economic perspective, but there are differences in the vocabulary of the two approaches which foreshadow differences of opinion on their starting points. The American aim is to *maintain*, preserve their existing leader position, while the European aim is to *ensure*, to strengthen European presence in AI research and development.

4. Major differences

Despite the common economic approach, there are major differences between the US and the European regulation of AI. This part of our paper attempts to

9 See e. g. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October of 2022; Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022.

10 American Artificial Intelligence Initiative: Year One Annual Report (hereinafter: Annual Report). Washington, The White House, 2020. 1.

11 See Communication II op. cit. 2–5.

illustrate these differences in a compact, yet thorough manner by presenting the strategic materials and legislation already briefly mentioned above.

4.1. The definitions of AI

First and foremost, we ought to start with the concept of AI, as the definition of the regulatory subject reveals the main characteristics that the legislator considers essential. Given that AI is a global technological product, the optimal case would be to use a universally accepted concept. Unfortunately, reality is different – as the plural case of "definitions" used in the title of this subparagraph indicates. Although AI will surely have an increasing impact on the lives of people in the future, it seems that all competent actors are creating their own definitions and it is not uncommon to use multiple concepts simultaneously, which complicates the situation for both future legislators and enforcers.

In the US, we have many different definitions for AI. For example, the Department of Homeland Security's document defines AI as "automated, machine-based technologies that have at least some self-direction capability and are capable of making predictions, recommendations, or decisions that affect the real or virtual environment for a given human-defined set of objectives."[12] However, the AI Initiative Act has a different definition for AI worded as

> "a machine-based system capable of making predictions, recommendations, or decisions affecting the real or virtual environment for a given set of human-defined goals. AI systems use machine- and human-based inputs to (A) sense the real and virtual environment; (B) automatically abstract these senses into models through analysis; and (C) formulate information or action options using the model's inferences."[13]

However, this statutory definition is not exclusive in US law, as a prior law provision for fiscal year 2019 again used a different definition.[14] This is significant because, for example, the AI Training Act, which aims to prepare

12 US Department of Homeland Security, Artificial Intelligence Strategy, 2020, 1.

13 National Artificial Intelligence Initiative Act of 2020, section 5002. (3).

14 See John S. McCain National Defense Authorization Act for Fiscal Year 2019, section 238 (g).

the workforce for working together with AI uses the latter definition.[15] Finally, it is also worth mentioning that the Blueprint introduces and uses the definition of automated system instead of AI.[16] The common point of these definitions is that AI is seen as an automated technology, operating based on human inputs but without human oversight, which is able to manipulate its environment, make predictions, decisions and recommendations in a human-like way. Besides the definition of AI, we must also mention the definition of AI system as well which is "an engineered or machine-based system that can, for a given set of objectives, generate outputs as predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy."[17] From the US approach, we can conclude that AI is a technology capable of performing a wide range of human-like actions in support of human activity.

The EU conceptual framework is also as diverse as the US one. Similarly to the US, the EU has several competing concepts in the literature. According to the EU's AI Strategy, AI "refers to systems that display intelligent behaviour by analysing their environment and taking action – with some degree of autonomy – to achieve specific goals."[18] The proposed regulation published by the EC, similarly to the Blueprint published in the US, does not include a specific definition of AI, but introduces the term AI system instead, which is a "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with." The European Parliament proposed to change this definition to the following: an AI system is "a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments."[19] The European approach, similarly to the US approach, includes manipulation of the environment, whereby AI performs its activities in order to achieve certain objectives, such as making recommendations or decisions. It is interesting that in earlier professional reports, autonomy can be found as a defining characteristic

15 AI Training Act section 2 (a) (1).

16 White House, Blueprint for an AI Bill of Rights, 2022, 10.'

17 National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, 2023, https://doi.org./10.6028/NIST.AI.100-1, (hereinafter: AI RMF 1.0) 4.

18 Communication I op. cit. 1.; Communication II op. cit. 1.

19 European Parliament P9_TA(2023)0236 Amendment 165.

of AI, while the original proposal of the EC did not include this in the proposed regulation. The European Parliament however also considered it necessary to include autonomy among the elements of the definition.

4.2. American legal framework

As it was mentioned earlier, the main aim of US regulations is ensuring US leadership in AI R&D. In 2022 alone, the National Science Foundation[20] earmarked more than $850 million for this purpose.[21]

However, achieving this goal does not mean that the US will give up its system of legal acquis. The expectations for AI are transparency, trustworthiness, that it should be explainable[22], and that there should be safeguards that guarantee robustness and resilience.

However, these requirements are currently not fully met.[23] In defining the US legal framework, it is important to emphasise the view that there are also limits which aim to uphold civil rights, civil liberties and privacy.[24] This is reinforced by Executive Order 13859, which stated that R&D involving AI must be conducted in a manner that maintains safety, security, privacy and confidentiality consistent with applicable laws and policies.[25]

Existing US legislation can be grouped into two categories. On the one hand, some rules (such as the prohibition of discrimination in labour law) are essentially technology-neutral, thus these must be adhered to even if AI is used in work processes. On the other hand, there are regulations that are technology-sensitive. In this area, one can find norms that may be legally questionable when AI devices are concerned (for example in the case of self-driving vehicles). The main challenge in creating or amending the legal norms in this case is that we do not currently have all the data we need to assess the real social impact of the risks inherent in AI. This is significant because the prevailing view in US legislation is that it is not prudent to regulate against imagined harms.

---

[20] The National Science Foundation (NFS) is a federal government agency whose mission is to provide funds for scientific research.

[21] Annual Report op. cit. 4–5.

[22] Select Committee on Artificial Intelligence, The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update, 2019. 19.

[23] Annual Report op. cit. 6–8.

[24] Ibid. 1.

[25] Executive Order 13859 of February 11, 2019 (EO 13859), Section 2 (b)–(c).

Three main objectives regarding AI have already been identified for legislation: ensure public engagement, limit regulatory overreach, and promote the trustworthiness of AI.[26] In a professional report, the main characteristics ensuring the trustworthiness of AI systems were defined. According to this, an AI system must be valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced and fair without harmful bias. These characteristics complement and reinforce each other, forming a coherent framework[27] In order to reach reassuring answers to the legislative questions and enhance their AI capacity, the US Department of Justice set in place its own AI strategy.[28]

4.2.1. Legislation

In contrast to the European legal framework, the US has several legal provisions that deal with AI. First of all, Executive Order 13859 (hereinafter: EO 13859) set out the principles of the AI Initiative Act, namely: ensuring scientific breakthroughs; ensuring development standards and safe testing for the benefit of US industry; preparing US workers for the spread of AI-based technologies; building trust by protecting US values, civil liberties and privacy; and creating the right international environment. The right environment is, of course, envisioned as one that provides markets for American results in AI development.[29]

The main purpose of the AI Initiative Act is to provide organizational and financial structure. This is ensured by the National Science and Technology (NST)[30] through the Select Committee on Artificial Intelligence established by EO 13859.[31] One of the expectations of the Executive Order was to prepare a memorandum to examine the legislative situation, while also paying special attention to reducing barriers. Within 180 days of the publication of the memorandum, agencies with legislative authority were required to review their authority over AI and submit the results to OMB tasked with providing

[26] Annual Report op. cit. 13–15.

[27] AI RMF 1.0 op. cit. 12.

[28] U.S. Department of Justice, Artificial Intelligence Strategy for the U.S. Department of Justice, 10–11.

[29] EO 13859 op. cit. Section 1.

[30] National Science and Technology is a coordinating and advisory body established by Executive Order 12881.

[31] EO 13859 op. cit. Section 3.

regulatory consistency by compounding the reviews and their results.[32] In other words, EO 13859, in addition to providing an organizational structure, took a major step toward coordinated, federal-level rulemaking on AI.

The main point of the Memorandum of the OMB is that AI innovation should not be made unnecessarily difficult.[33] This position is fully in line with economic considerations – it seems clear that the US regulatory approach, while taking ethical questions and fundamental rights into account, cannot break away from a purely economic logic for regulation.

It is therefore no coincidence that the memorandum envisages legislation that will help identify potential risks[34] and respond to them in a way that will improve the global competitiveness of US firms. For this reason, federal agencies should refrain from setting standards that are too high, both because they would prevent society from reaping the full benefits of AI and because they could negatively affect US competitiveness.[35] In this context, however, the question rightly arises as to what extent such a preference for the economic aspect would undermine fundamental rights or the liability regimes in the future and to what extent this would undermine consumer protection rules.

The memorandum sets out ten principles to be considered for legislation. The first principle is public trust in AI, which presupposes the existence of reliable and stable AI applications. In this context, the nature of the risk must be considered when setting the standards, as it determines the scope and force of the intervention. The second principle is public participation, which implies adequate information given to and the involvement of society. The third principle is scientific integrity and information quality. In this context, the strengths and weaknesses of the application of a given AI must be assessed during the legislative process. The fourth principle is risk assessment and management. This does not mean that all foreseeable risks should be mitigated, as the American legal position is that all activities involve trade-offs, and therefore a risk-based approach (weighing up the benefits and drawbacks) to codification is justified. The normative basis for assessing risk is provided by Executive Order 12866. One of the main purposes of this principle is to

32 EO 13859 op. cit. Section 6.

33 Office of Management and Budget, Memorandum M-21-06, 2020 (hereinafter: Memorandum), 2.

34 Identifying the potential risks are important step because the negative impacts of risks related to use of AI systems can be experienced by wide range of people as it was mentioned in AI RMF 1.0 op. cit. 4.

35 Memorandum op. cit. 2.

eliminate two extreme legislative approaches (hazard-based vs unnecessarily precautionary), thus ensuring a justiciable and competitive regulation. The fifth principle is called benefits and costs. Its starting point is the recognition that the increasing use of AI may raise specific issues that have not been addressed *a priori* by the legislator. Closely linked to this, there is a passage in Executive Order 12866, which requires that social costs and benefits should always be considered when legislating. This principle imposes a duty of discretion on the legislator in this respect. The sixth principle is flexibility, which states that it is inappropriate to legislate in a way that is from the start already too rigid in regulating certain technological specifications of AI, as this will result in impractical and ineffective regulation. In the regulatory arena, attention should be paid to the international use of AI to ensure US competitiveness. The seventh principle is fairness and non-discrimination. The basis of this principle is that AI can be used to reduce discrimination, but existing real-world biases can also influence the decisions made by AI. This should be considered in the norm-setting process. The eighth principle is disclosure and transparency. The importance of this lies in building trust, as openness and transparency can increase the general public's understanding of how AI works, while also letting experts understand the process by which the AI has made its decisions. The ninth principle is safety and security. In this context, future legislation should consider potential security risks, vulnerabilities, and malicious deployment. The last principle is interagency coordination. This principle is laid down to promote agency interaction under Executive Order 12866 to ensure a coherent and holistic whole-of-government approach.[36]

The risk assessment process highlights the importance of risk management. In this respect, the US considers a risk management approach that covers the entire life cycle of the AI system. In this context, the professional report titled Artificial Intelligence Risk Management Framework (Version 1.0) (AI RMF 1.0) introduces the 'Core steps', which include four functions (govern, map, measure and manage), that make up the procedural protocols for the risk assessment and for the full context analysis and measurement. Based on the information and data gathered, it is possible to prioritise risks and monitor them accordingly. This process is supported by various profiles that assist decision-making.[37]

From the law that already exists, a special mention should be made of Executive Order 13960, which promotes the use of AI (when it is considered appropriate)

[36] Memorandum op. cit. 2. 3–7.

[37] AI RMF 1.0 op. cit. 20–34.

in federal government agencies, as it can be a useful tool for building public trust.[38] In this context, the Executive Order articulates nine principles that should be applied when the US government uses AI. Based on these principles, the use of AI should be lawful and respectful of the Nation's values; purposeful and performance-driven, accurate, reliable, and effective; while the AI system should also be safe, secure, and resilient; understandable; responsible and traceable; regularly monitored; and transparent and accountable.[39]

Other examples of legislation that also contain provisions on the development and use of AI include the AI Training Act, the AI in Government Act, and the Advancing American AI Act. Finally, it should be noted that US legislation is not only about legislation itself, but it also supports the use of soft law instruments such as guidelines, ethical directives, frameworks, pilot programmes and experiments. Some agencies of the US government have already made use of such soft law instruments.[40]

The possibility of using soft law tools stems from the fact that when an AI tool acts autonomously, it is expected to comply with formal and informal norms just as humans are also expected to do. This is also the basis of the need to explore ethical, legal, and social implications of AI.[41]

In this context, we should mention the latest Executive Order (EO 14110) connected to this topic, which was issued 30th October 2023. It confirmed the views that promoting the responsible use of AI is justified as the only way to create a productive, innovative, and safe environment. This is also important because the irresponsible use of AI exacerbates societal harms such as disinformation, bias, discrimination, and fraud, while it may also displace and disempower workers, stifle competition, and pose risks to national security.[42]

Eight principles were defined to enable the responsible use of AI. The use must be safe and secure which means an AI must be robust and reliable, its processes must be repeatable, and it must contain standardised evaluation. To meet these expectations, the risks of the AI must be tested and mitigated. Last but not least, American citizens also have the right to be made aware if and when they use an AI-based device or service. The second principle is the promotion of responsible innovation, competition, and collaboration. This

38 Executive Order 13960 of December 3, 2020 (hereinafter: EO 13960), Section 1. (3).

39 EO 13960 op. cit. Section 3. (3).

40 EO 13960 op. cit. Section 1. (4).

41 Select Committee on Artificial Intelligence, The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update, 2019, 20.

42 Executive Order 14110 of October 30, 2023 (hereinafter: EO 14110) Section 1.

principle lays down the basis for using the potential of technology and solving societal problems. It focuses on training, education, promoting research and supporting small businesses and workers. The third principle is the responsible development and use of AI, based on the idea that the rise of AI should not lead to negative changes in the labour market and that the integration of workers' and trade unions' views and rights should be supported. The fourth principle is that AI policies must be consistent in advancing equity and civil rights. Discrimination and bias may occur when AI is used, the effect of which can be further increased by irresponsible use. To prevent this, Executive Order 14110 has reinforced the relevant requirements of the Blueprint, of the AI RMF 1.0 and of Executive Order 14091. The fifth principle is the adequate protection of the interests of Americans when they purchase and use AI products. This principle highlights the importance of consumer protection in the face of current technological change. The sixth principle focuses on adequately protecting Americans' privacy, personal data, information, and civil liberties. The seventh principle concerns the responsible use of AI in government. This includes an expectation to involve AI professionals as much as possible. The last principle encompasses the objective of ensuring the dominant role of the United States, which requires the development of a global framework for risk management.[43]

Executive Order 14110 also introduced the definition of AI model, which refers to *a component of an information system that implements AI technology and uses computational, statistical, or machine-learning techniques to produce outputs from a given set of inputs*. A further concept in the field of risk management is "AI red-teaming", which aims to find flaws and vulnerabilities in AI systems, including unforeseen or undesirable system behaviours or risks arising from the misuse of the system.[44] Also worth mentioning is the notion of "AI system", which refers to any data system, software, hardware, application, tool, or utility that operates in part or in whole using AI.[45] Executive Order 14110 has set deadlines for the bodies of the Administration in order to achieve the objectives and to enforce the principles.

[43] EO 14110 op. cit. Section 2 (a)–(h).

[44] Ibid Section 3 (c)–(d).

[45] Ibid. Section 3 (e).

4.2.2. Blueprint

When analysing the US's regulation of AI, it is not sufficient to look at existing legislation, as the White House released the Blueprint in October 2022, which comprehensively addresses legislative issues connected to AI.

The starting point for the Blueprint is that existing law provides protection in several specific areas. This may need to be supplemented, however, standard-setting at the federal level should not lose sight of the fact that some legislation has already been enacted at the state level.[46]

In the context of standard setting, the Blueprint also makes statements of principle, with a specific mention of the US acceptance of the OECD Recommendation which contains principles for AI.[47] It also considered the principles of the 1973 Fair Information Practice Principles (FIPPs).[48] Overall, the Blueprint included five principles and additional complementary practices to guide design, use and deployment.

The first principle set by the Blueprint is the safety and effectiveness of AI systems. This principle promotes the involvement of as many stakeholders as possible to identify risks and explore the potential impacts of systems. In principle, it is the responsibility of developers and users to lay out a clear governance structure and procedures. This includes governance procedures before deployment and the responsibility of individuals and bodies that oversee assessment and mitigation throughout the life cycle of the system. Responsibilities should be sufficiently well-detailed to ensure safety. Independent assessment processes and regularly updated reports are needed too.[49]

The second principle deals with the issues of protection against algorithmic discrimination: avoiding this is an important aspect, and the professional report therefore expects increased activity in this area from designers, developers and deployers.[50]

The third principle is data privacy, which is important because it involves a wide range of threats. Under this principal data protection, risks must be

46 White House, Blueprint for an AI Bill of Rights, 2022, (hereinafter: Blueprint) 9.

47 OECD, Recommendation of the Council on Artificial Intelligence.

48 Blueprint op. cit. 9.

49 Ibid. 15–22.

50 Ibid. 5.

assessed throughout the life cycle of the system and private data must be used only to the necessary extent.[51]

The fourth principle is proper notice and explanation, which places a strong expectation on stakeholders to notify users when an automated system is being used.[52] In itself, this requirement for adequate information is not new, as the professional report indicates that it is already required by several active legislations. Proper notification about automated systems is important because these systems can affect the rights, opportunities, and access of individuals. The notification should explain how the system and its decision-making mechanism works in plain terms. To ensure accountability, the person or body responsible should be clearly identified. In addition, the principle also requires an appropriate risk assessment and recommends that explanatory mechanisms should be built into the system design to explain the overall behaviour of the system.

The fifth principle is about human alternatives, consideration, and fallback. This principle implies the necessity of a human backup system as fallback. An automated system can break down at any time, which is why the Blueprint gives Americans the right to human review. Healthcare and the criminal justice system is specifically mentioned in this context. There are already several areas where AI is being used, but the professional report argues that the use of technology can lead to risks in the absence of appropriate safeguards.[53]

4.3. EU legal framework

When looking at the US and European legal framework, two main differences can be identified. One is the lack of regulation at the European normative level. This is the reason why, at the time of writing this paper, we are not yet able to list any relevant AI-focused legal regulations of the EU. We are currently awaiting the adoption of the proposed regulations and directives put forward by the EC.

Looking at the legislative trends that are emerging, another difference can be found between the US and the EU, namely the extent of regulation. US legislation is characterised by restraint and avoiding overregulation. Other features in the US are case-by regulation, such as regulation on the government

[51] Ibid. 30–39.

[52] Ibid. 40–45.

[53] Ibid. 46–52.

use of AI, trainings in AI, the financial and organisational structure for research and development, and regulatory principles at the normative level. In contrast, the EU legislative approach is to regulate the main issues affecting AI in a comprehensive manner by means of regulations and directives, while the principles governing the regulation have so far been set out in professional documents rather than in normative texts.

4.3.1. Regulatory principles

The key aspects guiding EU legislation can be found in the AI Strategy, the EC's White Paper and the HLEG guidelines. The AI Strategy took a two-level strategic approach, as it required Member States to develop their own national strategies in addition to the approach set globally for the EU.[54] The EU-level strategy, similarly to the US approach, focused on competitiveness, and more specifically on strengthening it. This was to ensure the EU's dominant role in the increasingly fierce global competition in the field of AI.[55] The strengthening of positions is linked to the issue of databases, as AI technology is extremely data intensive. If data were not available in sufficient quantity and quality, Europe would be left behind in research and development. For this reason, the EC considered it essential to provide data without detriment to existing data protection legislation, including the relevant provisions of the GDPR.[56] The AI Strategy considered it appropriate to have an ethical basis for regulatory issues. There is a strong normative basis for a European ethical approach, which is based on, among others, the Charter of Fundamental Rights of the European Union.[57] Another important argument in favour of an ethical approach was that the existence of ethical AI ensures that AI is also human-centred.[58] In both the US and EU contexts, the inclusion of ethical considerations is interesting, as the regulatory concept is based on strengthening competitiveness – this is particularly striking in the US context. The extent to which ethical considerations can be acknowledged in legislation aimed at optimising competitiveness is intriguing from the practical implementation of regulation point of view.

54 Communication I op. cit. 3.

55 Communication II op. cit. 2.

56 Communication I op. cit. 7.; Communication II op. cit. 12–13.

57 Communication II. op. cit. 18.

58 Communication I op. cit. Annex 1.

The EC's White Paper stressed that in the case of the EU, there is no lack of regulation, as the developers and users of AI must comply with the legal requirements in force.[59] Indeed, to this extent, our earlier assertion concerning the lack of normative regulation should be reconsidered. There is no doubt that there is no specific EU legislation on AI in force yet, but the existing body of law does affect development, research, and use – however, our point is correct in that while the US already has specific legislation on AI, the EU does not.

The White Paper foreshadowed one of the most important elements of the subsequent proposal for a regulation: a risk-based approach. The main concerns about AI are that its operation is opaque and unpredictable,[60] which may erode trust. We also find similarities with US regulation in this respect. Both blocs have identified the goal of increasing trust, and both see that this trust can be eroded by unclear and unpredictable operations, i.e., regulation is needed to address these concerns.

Another common point is that the EC does not support a regulation setting that is overly prescriptive. The starting point is that legislative intervention is only necessary where the risk is high.[61] The White Paper has introduced significant risk as a new definition. According to this, a multi-stage risk assessment is necessary, which as a first step identifies the sectors where there is a significant risk on a sector-specific basis. The next step would be to carry out a repeat risk assessment within the risk-affected sectors in the context of AI applications, whereupon EU regulation would have to cover the AI applications that have a significant risk. The next step would be individual exemptions. For those AI applications that would not be covered by the proposed EU regulation, the possibility of a voluntary labelling scheme would be upheld, which would still result in the use of the legal provisions set by the EU. Another possibility for actors in this field is to introduce their own set of rules, similar to the proposed EU regulation. The main goal of these steps and opportunities is to enhance confidence.[62]

It is also worth mentioning the HLEG ethical guidelines supporting the work of the EC, which were also formulated based on the concept of trustworthy AI. According to the expert group, AI is only trustworthy if it is robust, used

[59] European Commission COM(2020) 65 final, White Paper on Artificial Intelligence – A European Approach to excellence and trust (hereinafter: White Paper), 12.

[60] Ibid. 14–15.

[61] Ibid. 21.

[62] Ibid. 22–29.

lawfully and ethically,[63] and has been associated with fundamental rights aspects such as human dignity, the guarantee of individual liberty, the rule of law and democracy, equality and solidarity, and civil rights.[64] On this basis, the HLEG has identified four ethical principles: respect for human autonomy, prevention of harm, fairness and accountability.[65] It is worth mentioning that there are overlaps between fundamental rights and ethical principles and, as the expert group pointed out, there may be competition between the principles in terms of their application.[66]

5. Conclusions

In summary, our comparison shows that US and EU legislators have quite similar views about many aspects of AI regulation (e.g., competitiveness, reliability, ethical considerations, respect for existing fundamental rights, avoidance of over-regulation). There is certainly a legislative and societal need for a robust legislation, while the difference between these two blocs of states basically lies more in the choice of values which defines the extent and scope of the regulation.

Currently, the US already has specific legislation on AI, as well as a financial and organisational structure for research and development. In contrast, the EU does not yet have such a structure, but this should not be interpreted as a "*backlog"*, since on the one hand the EC proposals for regulations and directives will be adopted in the near future and on the other hand the normative basis foresees the establishment of a known and proven governance structure. In the legislative field, the fundamental difference is that the EU plans to introduce a holistic regulation, whereas the US is more a case-by one.

There is also an evident specific duality in both the US and the EU: on the one hand, there is a very strong economic perspective, which sees AI primarily as a technology that can contribute to improving competitiveness and to gaining new markets. The regulatory logic is closely linked to this, since both blocs clearly stated that over-regulation should be avoided, and legislation should only be enacted if and to the extent that it does not constitute an economic obstacle.

[63] High-Level Expert Group on AI presented Ethics Guidelines for Trustworthy Artificial Intelligence (HLEG Guidelines) 2–10.

[64] Ibid. 13–14.

[65] Ibid. 14–16.

[66] Ibid. 16–17.

On the other hand, legislators are also seriously concerned with issues of trust and human-centred design, which inevitably lead to ethical considerations and fundamental legal questions. A direct consequence of this is the extremely precise principal structure that underpins both American and European legislative concepts. This dichotomy can be seen in the professional reports, where the economic aspect, which seeks to minimise regulation, meets with existing fundamental rights protections and ethical principles that reinforce trust. The EU has taken a decisive step in the latter direction, while the case-by regulation in the US has not yet clearly moved in either direction, but the latest Executive Order (EO 14110) shows similar steps taken towards a comprehensive regulation.

When comparing these two blocs, it is important to underline again that the American economic approach is to strengthen their leadership, while the European one aims to acquire that leadership. This is interesting because, despite their common values and necessary cooperation in global scale, the two blocs are also natural adversaries in the pursuit of their economic goals.

All in all, we can remarque that one of the advantages of European holistic regulation seems to be its comprehensive approach, which treats the subject of regulation as a closed, coherent system. The creation of such a structure may also provide greater scope for fundamental rights or ethical considerations. However, this structure may make it more difficult to respond to the changes that are a feature of technological innovation. Another disadvantage of a complex regulatory system could be the increased market entry costs due to regulatory compliance, which could adversely affect small and medium-sized enterprises, which could lead to the introduction of a targeted EU aid scheme to improve the competitiveness of European enterprises in the global market.

In this respect, the specific US regulatory approach seems to be more flexible in relation to technological innovations, as it requires only to change some specific detailed rules. At the same time, the nature of a specific regulation may, in practice, raise doubts about the effective appearance of the fundamental rights and ethical considerations that legislators advocate.