Luiss
Policy Observatory

EU and US regulatory approach to AI: a comparative perspective

By Camilla Scarpellino[1]

Policy paper n. 10/2024

The purpose of this paper is to examine and compare the regulatory frameworks for artificial intelligence (AI) in the European Union and the United States. The study starts from the current legal framework of those jurisdiction: the European Union's AI Act and the United States' Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (EO). It analyzes the legal structures, the overarching objectives, the governance and oversight mechanisms, and the expected outcomes of each legal solution. The AI Act is a comprehensive regulation on AI tools, which is binding across all EU member states. It adopts a risk-based approach to ensure the safety and accountability of AI systems. On the other hand, the US Executive Order promotes flexible guidelines and collaborative standards, as it fosters and protects innovation while safeguarding public welfare and individual rights. The paper wants to discuss the implications of the two approaches for global AI governance and technological advancement, comparing the shared goals and the divergent strategies of the two frameworks. Finally, recommendations are suggested for future AI policies initiatives in the EU, emphasizing the importance and the possible role of harmonized standards, workforce training, and international cooperation to foster a secure and innovative development of AI systems.

[1] Coordinatrice del Policy Observatory, Ph.D. Candidate in Law and Business.

Introduction

Both the EU and the US have recently adopted AI regulations, respectively the AI Act and the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (EO). Those two acts show different approaches to the governance and regulation of AI. The main difference can be observed precisely in the choice of the regulatory tool. In fact, the AI Act is an imperative legal provision proposed by the European Commission in April 2021, later discussed by the co-legislators, the European Parliament and the Council, and finally endorsed by the European Parliament through the AI Act in March 2024. The regulation is directly applicable to all Member States, becoming legally binding two years after its publication in the Official Journal of the European Union. Instead, Executive Orders are directives issued by the President of the United States; thus, they carry the force of law and can affect policy and governance without requiring approval from Congress. This paper analyzes similarities and differences between these two regulations in the following order: the legal framework overall, the scope and purpose, the governance and oversight system, and, finally, the goals pursued under each framework.

A general overview of the AI Act and the Executive Order

The AI Act seeks to harmonize the rules applicable to all AI systems that are going to be placed on the European market in order to ensure trustworthy AI products. It provides a regulatory framework that lays down mandatory requirements and obligations that AI systems should fulfill to be legally introduced and traded within the EU. Therefore, its scope regulates the activities of all operators involved in the AI value chain, such as developers, providers, and users. The Act will be completed by a set of harmonized standards based on a standardization request issued by the European Commission, in consultation with European Standardisation Organisations (ESOs) and relevant stakeholders. This request should also include other aspects of AI governance systems, such as provisions on reporting and information to enhance AI systems' performance. Finally, coordination is delegated to at least one notifying authority and one market surveillance authority in each Member State. The notifying authority will be responsible for coordinating the bodies assessing AI devices' compliance with the AI Act and issuing the conformity certification required by AI operators to sell their devices and software in Europe. At the European level, the Act also establishes authorities and bodies engaged in the implementation of AI legislation and in the standardization processes.
On the other hand, the Executive Order highlights opportunities arising from AI in bolstering competitiveness, economic security, and technological leadership, with a strong emphasis on maintaining American leadership in AI innovation and its responsible utilization to enhance public welfare. The EO sets out eight guiding principles and priorities with a view to ensuring safety and security, promoting innovation and competition,

advancing equity and civil rights, and protecting privacy and civil liberties[2]. Its focus is on developing and introducing AI technologies across various sectors, emphasizing the role of federal agencies in taking the lead in this and safeguarding rights, but without setting specific risk levels and limitations associated with AI. The EO directs federal agencies to bolster AI enforcement, ensuring AI systems are secure and comply with the aforementioned principles. It emphasizes guidelines and standards rather than rigid rules and seeks collaboration with industrial and other stakeholders to develop these standards. Finally, the EO's oversight mechanism relies on an interagency body, the White House AI Council, tasked to "coordinate the activities of agencies across the Federal Government to ensure the effective formulation, development, communication, industry engagement related to, and timely implementation of AI-related policies, including policies set forth in the order"[3].

The Legal Framework on AI in Europe and the United States

The public's attention on the AI phenomenon had prompted Western governments to address its risks and limitations well before 2023. The European "AI innovation package" was preceded by various declarations and communications from European institutions. In fact, the first European attempt to regulate AI was the General Data Protection Regulation that requires the right to ask for human intervention or "the right to express his or her point of view and to contest the decision based solely on automated processing"[4]. In 2017 the European Council recognized the urgency to build a digital market in Europe, focusing on nine principal objectives: developing **e-government** and deploying new technologies in the public sector; issuing a future-oriented **regulatory framework**; building a **first rate infrastructure and communications network**; adopting a common approach to **cybersecurity**; combating **terrorism and online crime**; ensuring a trained and **educated workforce with digital skills**; supporting the industrial sector in the digital transition; **addressing the opportunities and the issues** arising from emerging technologies such as blockchain; and, finally, Artificial Intelligence[5]. The European Parliament responded by calling on the EU Commission to propose a regulatory framework on "Civil law rules on robotics" to address the damage and violations of rights caused by those recent and pervasive technologies[6]. The Parliament's Resolution suggested a public recording system for advanced smart robots exhibiting autonomous and cognitive features[7], and it assigned to the European

[2] Cit. Duane C. Pozza, Kathleen E. Scott, Kara M. Sacilotto, Lisa Rechden and Lauren N. Johnson, New Artificial Intelligence Executive Order from President Biden Outlines Sweeping Approach to AI, in The Computer & Internet Lawyer, 2024;

[3] The White House, Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 30 October 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/;

[4] Art. 22 of the GDPR;

[5] Cit. European Council meeting (19 October 2017) – Conclusions, Brussels, 19 October 2017, https://data.consilium.europa.eu/doc/document/ST-14-2017-INIT/en/pdf ;

[6] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL));

[7] Accordingly the above-mentioned Resolution considers robots smart if the software presents the following characteristics: the acquisition of autonomy through sensors and/or by exchanging data with its environment (inter-connectivity) and the trading and analyzing of those data, self-learning from experience and by interaction (optional criterion), at least a minor physical support, the adaptation of its behavior and actions to the environment, absence of life in the biological sense;

Commission the task of establishing those categories that needed registration, before placing them on the EU market.

On the other side of the Atlantic, the US path for AI regulation took an important step in October 2022, when the White House's Office of Science and Technology Policy published the "Blueprint for an AI Bill of Rights", addressing the "challenges posed by the use of technology, data, and automated systems, which can threaten the rights of the American public"[8]. The Blueprint focuses on the need for safeguards so that automated systems are safe, effective, and non-discriminatory. To this end, it proposes five principles that AI operators should follow to design and deploy automated systems in order to protect civil rights and democratic values. These include: ensuring the **safety** and **effectiveness** of AI systems; preventing **algorithmic discrimination**; **protecting data privacy**; providing notice and explanation to individuals impacted by automated systems; and offering **human alternatives and fallback options** such as ensuring "access to timely human consideration and remedy by a fallback and escalation process if an automated system fails, it produces an error, or you would like to appeal or contest its impacts on you"[9]. The aim is to guide the manufacture and development of automated systems that have the potential to impact individuals or communities' rights, opportunities, or access to critical resources or services, ensuring protection from algorithmic discrimination. In July 2023, President Biden announced the "Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by IA" that commits, on a voluntary basis, fifteen AI companies to ensure safe, secure, and trustworthy AI. In particular, these companies should commit to internal and external red-teaming of models or systems in sensitive areas[10], share information among companies and governments, invest in cybersecurity, incentivize third-party discovery and reporting of issues and vulnerabilities, label the digital contents generated by AI, publicly report model or system capabilities, limitations, and domains of appropriate and inappropriate use[11].

It is worth noting that Europe and the United States have both recognized the potential of the digital market, emphasizing the integration of new technologies in the public sector and enhancing global industrial capacity. Additionally, they share the same concerns about AI systems, including cybersecurity threats, data protection violations, and the risk of harmful bias and discrimination.

On the other hand, the two paths present differences on the approach to the industrial sector. Europe emphasizes the need to support new digital operators, strengthen infrastructure and the communications

[8] Cit OSTP – The White House, Blueprint for an AI Bill of Rights;

[9] Cit OSTP – The White House, Blueprint for an AI Bill of Rights on Human Alternatives, Consideration, and Fallback;

[10] Misuse, societal risks, and national security concerns, such as bio, cyber, and other safety areas;

[11] Cit. The White house, FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI, in https://www.whitehouse.gov/wp-content/uploads/2023/07/Ensuring-Safe-Secure-and-Trustworthy-AI.pdf ;

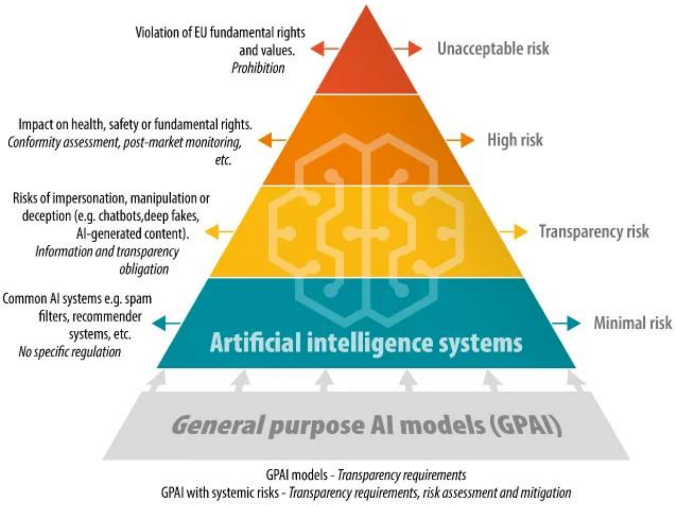
network, and develop the digital market, while the US is more committed to guiding “Big Tech” toward responsible innovation.

Scope and Addressees of the regulations

The AI Act addresses the regulation to developers, deployers, importers, and distributors of AI systems who want to place their system on the European market, while the EO addresses its obligations to executive departments and federal agencies. That is because the AI Act lays down a set of requirements for AI systems and obligations that AI operators should fulfill both during the AI manufacturing and development phase as well as following the commercialization of the system. The EO calls on federal agencies to cooperate and follow the principles and priorities set by the Order and comply with the tasks assigned to each administrative body to promote the safe, responsible and reliable development of AI. Those agencies are mentioned in various contexts within the EO, with tasks ranging from regulation and risk assessment to the promotion of innovation and international collaboration. The reason why the two regulations address different subjects is closely linked to the stage in the legislative process reached by EU and US digital regulation, the content, and the purposes of the laws, which this study is going to illustrate.

The Legal Framework

The AI Act's primary aim is to establish a general framework for AI governance, structured around a risk-based approach that categorizes AI systems into four risk levels: unacceptable, high, systemic, and minimal.


Violation of EU fundamental rights and values.
Prohibition
Unacceptable risk
Impact on health, safety or fundamental rights.
Conformity assessment, post-market monitoring, etc.
High risk
Risks of impersonation, manipulation or deception (e.g. chatbots,deep fakes, AI-generated content).
Information and transparency obligation
Transparency risk
Common AI systems e.g. spam filters, recommender systems, etc.
No specific regulation
Minimal risk
Artificial intelligence systems
General purpose AI models (GPAI)
GPAI models - *Transparency requirements*
GPAI with systemic risks - *Transparency requirements, risk assessment and mitigation*

Data source: European Commission

At the pyramid’s apex is the Unacceptable Risk category, encompassing all prohibited AI systems. These are defined by characteristics such as: subliminal techniques, intentionally manipulative or deceptive methods aimed at distorting the behavior of individuals or groups; social scoring and predictions regarding an individual's likelihood of committing a criminal offense; facial recognition used to infer emotions in workplace and educational settings; and biometric categorization systems capable of deducing personal qualities, opinions, or beliefs.[12].

High-Risk AI systems are those which "pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by materially influencing the outcome of decision making"[13]. These systems must meet specific technical requirements to ensure compliance:

- **A risk management system** capable of identifying and analyzing all foreseeable risks in order to mitigate or eliminate them (art. 9);
- **Data governance and management practices** for the data sets used during AI training, validation, or testing. These practices should address design choices, data collection processes, and the origin of data (art. 10).
- **Technical documentation** to demonstrate AI system compliance with these requirements (art. 11).
- **Automatic recording of events** ('logs') (art. 12).
- **Instructions for use**, including all relevant information about the AI's purposes, its level of accuracy, and any known or foreseeable circumstances that may pose a risk to fundamental rights (art. 13).
- Human-machine interface tools that enable **human oversight** of the systems (art. 14).
- **Benchmarks and measurement methodologies** to ensure an appropriate level of accuracy, robustness, and cybersecurity throughout the AI lifecycle (art. 15).

In addition to these requirements, the AI Act provides a set of obligations for high-risk AI providers, deployers, and other parties. These obligations are imposed on each operator involved in the manufacturing and distribution of AI systems to ensure that their systems are safe, accurate, and robust throughout their lifecycle. Consequently, AI systems must incorporate a quality management system that includes "examination, test and validation procedures to be carried out before, during and after the development of the high-risk AI system, and the frequency with which they have to be carried out"[14]. Moreover, operators must withdraw their systems from the market if they no longer conform to the AI Act. On the other side of the ocean, the Executive Order adopts a completely different approach, establishing **eight principles** to be implemented by administrative bodies through policy interventions that should consider "the views of other agencies, industry,

[12] Art. 5 of the AI Act - Text Adopted by the European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf

[13] Cit. Art. 6 of AI Act;

[14] Art. 17 of the AI Act text adopted;

members of academia, civil society, labor unions, international allies and partners, and other relevant organizations."[15]. These principles recommend:

1. Foster AI safety and security by developing guidelines, standards, and best practices, implementing effective monitoring mechanisms, and creating labeling systems to identify AI-generated content.
2. Promote innovation and competition through investments in education, research, and IP protection. Additionally, the US Government aims to equip its workforce with AI skills, attract global talent, and ensure a fair marketplace for small digital entrepreneurs while addressing risks posed by dominant firms in key technological domains.
3. Manage the impact of AI on the job market by training the workforce for the digital transition, ensuring that AI deployment in the workplace respects workers' rights, maintains job quality, and minimizes negative impacts on the workforce.
4. Promote policies that uphold equity and civil rights, rejecting any use of AI that perpetuates discrimination or bias.
5. Protect consumers, students, and patients by providing consumer protection laws to safeguard against fraud, bias, discrimination, and privacy infringements, especially in critical sectors like healthcare and finance, through an accountable AI system.
6. Ensure privacy protection by enforcing lawful, secure data practices and utilizing privacy-enhancing technologies to mitigate risks and safeguard against improper data collection and use, thereby protecting individual rights, including First Amendment freedoms.
7. Ensure responsible and effective AI governance by attracting and retaining AI professionals across various fields and communities to understand AI's benefits and risks, modernizing IT infrastructure, and adopting safe and ethical AI practices.
8. Strengthen American leadership in advanced technological innovation by developing responsible deployment frameworks and engaging with global allies to manage AI risks and promote common approaches to shared challenges[16].

The Executive Order entrusts departments and federal agencies with implementing these principles by identifying the foreseeable risks associated with AI use within their jurisdictions and suggesting measures to mitigate these risks, while also developing relevant guidelines and standards. Additionally, competent authorities will handle the training of AI expertise while safeguarding the current workforce, promoting AI

[15] cit. Sec. 2. Policy and Principles of the Executive Order;

[16] Duane C. Pozza, Kathleen E. Scott, Kara M. Sacilotto, Lisa Rechden and Lauren N. Johnson, New Artificial Intelligence Executive Order from President Biden Outlines Sweeping Approach to AI, Op. cit.;

research, and enhancing access to federal data sets. They will also focus on promoting data protection and fostering international cooperation.

AI Governance and Oversight

The EU's proposed AI governance system is based on a centralized approach involving European institutions, national authorities, and certifying bodies. Simultaneously, it mandates timely cooperation among all AI operators, identified as the manufacturer, deployer, importer, and users of the AI product. Specifically, "each Member State shall designate or establish at least one **Notifying Authority** responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of **conformity assessment bodies** and for their monitoring"[17]. They must verify that these bodies meet certain requirements and standards, ensuring they manage and maintain the independence, objectivity, and impartiality of their activities to prevent conflicts of interest. The Notifying Authority is also tasked with notifying the Commission and other Member States of each conformity assessment body. Conversely, the conformity assessment bodies are private organizations with legal personality that must meet the organizational and administrative operational requirements (i.e. quality management, human and economic resources) necessary to carry out their tasks (art. 31). They are responsible for assessing and certifying high-risk AI systems' compliance with the AI Act and standards; they must also communicate to the Notifying Authority any refusal, suspension, withdrawal, or limitation of a certificate (art. 45). They must operate independently; therefore, they are not allowed to offer consultancy services that could conflict with their assessment duties. Finally, each Member State shall establish or designate at least one Market Surveillance Authority to act as a single point of contact for the implementation of the AI Act (art. 70).

The AI Act's oversight activity is integrated with disclosure and transparency duties for providers, deployers, and manufacturers. One such duty is to perform a Fundamental Rights Impact Assessment to identify and evaluate the potential impacts of the AI system on safety and fundamental rights[18]. Further disclosure duties are established throughout the AI lifecycle. Deployers must monitor the operation of high-risk AI systems, keep records of any incidents, and communicate them to the competent authorities[19].

On the other hand, the EO's AI governance system is based on the analysis of AI risks and opportunities conducted by each Administrative Body, in their specific field of expertise; below are the main tasks of each agency:

[17] Art. 28 of the AI Act;

[18] The Fundamental Rights Impact Assessment also includes: a compliance check of the software as regards the AI Act's conditions, information on the data governance system and on the test and validation system employed;

[19] Art. 26 of the AI Act;

- Secretary of Commerce: advancing responsible global technical standards for AI development and use, and leading efforts to promote and develop AI standards in collaboration with international partners. The Department must establish a plan for global engagement on AI standards[20];
- Secretary of Energy: developing and implementing plans to foster AI model evaluation tools in the energy sector [21];
- Secretary of Homeland Security: assessing the risks associated with the use of AI in critical infrastructures and developing strategies to mitigate these risks. It is responsible for developing safety and security guidelines for critical infrastructure owners and operators[22];
- National Institute of Standards and Technology (NIST): developing resources and benchmarks for AI safety evaluation, and establishing guidelines to promote consensus industry standards[23];
- Secretary of Defense: engaging in pilot projects for using AI in cybersecurity and national security. It must develop plans to identify, develop, test, evaluate, and deploy AI capabilities that assist in discovering and remedying vulnerabilities in US government software, systems, and networks;
- Secretary of State: collaborating with international allies to develop standards shared on a global scale[24].

The EO also involves other agencies in the fields of national security, consumer protection, research, and labor policies. The Order appears to address the concerns raised by AI experts regarding short-term dangers such as bias, discrimination, and the more unpredictable long-term effects on the job market.

The oversight mechanisms provided in the two regulations are significantly different. The AI Act adopts a centralized approach, initially relying on providers' Risk/Impact Assessments and private certification. This process then moves to the National Authority, which coordinates and oversees the activities and status of the certification bodies responsible for issuing these certificates. Conversely, the EO relies on designated agencies to study and report on AI issues in critical infrastructure, cybersecurity, and chemical, biological, radiological, and nuclear (CBRN) threats. The work of these agencies is supervised by the AI Council, an interagency body established by the White House to coordinate AI policy across the federal government[25]. The Council gathers

[20] Sec. 11 lett. B of the Executive Order, according to that section the standards may involve AI nomenclature, best practices for data handling, trustworthiness of AI systems, and AI risk management;

[21] Sec 4.1 lett. B;

[22] Sec 4.3. Managing AI in Critical Infrastructure and in Cybersecurity lett. A;

[23] Sec. 4. Ensuring the Safety and Security of AI Technology;

[24] Sec. 11. Strengthening American Leadership Abroad;

[25] Sec. 12 Implementation;

the top officials of the federal departments and agencies tasked with supervising the implementation of AI policies[26].

Lastly, the AI Act also establishes the AI Office, a specific body to oversee the implementation of the AI Act across the EU. The Office advises the Commission, facilitates cooperation among national supervisory authorities, and provides opinions, recommendations, and best practices for implementing the regulation. It also contributes to cooperation among National Authorities and attends the European AI Board's meetings, which is composed of one representative per Member State, and oversees the AI Act's implementation among competent national authorities[27].

Conclusions and recommendations

In light of the brief analysis conducted on the two AI regulations, a common path can be observed between the US and the EU, despite differences in legal background, scope of application, and oversight systems. Indeed, the content of the two regulations is similar; they both stress the importance of protecting values such as health, safety, democracy, and the rule of law while recognizing the need to foster and support technological innovation. The primary difference between the two regulations lies in their approaches: the AI Act opts for a human rights-centric approach, while the EO emphasizes the need to support small businesses, startups, and entrepreneurs, as well as to train managers and the workforce to maintain American leadership in the tech sector. These differing goals explain the choice of legal tools and scope of application. The European Parliament seeks to impose legal obligations upon all AI operators involved in the AI lifecycle. In contrast, the EO has been careful not to constrain AI players within a rigid regulatory framework that could hinder the development of innovative software.

It is worth noting that the AI Act's rules are quite flexible, requiring technical specifications such as standards, guidelines, and best practices for their implementation. Articles 17, 31, and 32 specifically refer to these standards. The importance of harmonized standards is emphasized also in Article 40, which outlines a specific process for developing these standards involving EU institutions, such as the EU Commission and National Standards Bodies (NSBs), while considering the interests of relevant stakeholders represented in European stakeholder organizations[28]. The legal framework is not fully settled, much like the US AI governance system, which is currently awaiting reports from administrative bodies on the risks and opportunities of AI systems.

[26] The White House, Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 30 October 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ ;

[27] Art. 66 of the AI Act;

[28] EU Artificial Intelligence Act , Standard Setting, in https://artificialintelligenceact.eu/standard-setting/;

Given the common purposes of both legal frameworks, the different strategies adopted, and the varying degrees of innovation in the EU and US digital markets, we can offer the following recommendations for the next steps in AI governance in the EU:

- training the current workforce in data usage and associated risks, as well as preparing the next generation of EU workers through specific courses in data analysis and computer science. This includes providing internship programs to ensure practical training and work experience for undergraduate students. Specific computer science courses should also be provided in all faculties to foster horizontal coding skills and the use of data across various economic sectors;
- developing a European migration policy to foster research in tech fields and attract AI talent from other countries. This policy should map the distribution of digital skills across Member States and provide incentives in those with lower rates of STEM graduates and AI experts. Universities should recruit current AI experts and workers to train the next generation of students [29];
- building university-industry collaborations to ensure a better match between students' curricula and training and industry standards, thereby fostering a virtuous cycle between education and the job market[30];
- developing trustworthy AI requires expertise not only from the scientific field but also from social sciences. These experts are essential in identifying the individual and social impacts of each AI system and in helping programmers and developers improve algorithm fairness and bias remedies;
- providing an attractive environment for AI tech industries through a clear legal AI framework, informing AI operators about the legal responsibilities and obligations required in the EU market. A clear and stable legal framework can support industries much better than a legal system that does not provide a frame for AI issues, as it can prevent unexpected lawsuits and high payouts[31]. Regulatory sandboxes can be an important legal tool to prepare SMEs and Big Tech operators to integrate easily into the EU digital market[32];
- fostering competition between companies providing "foundation" models, which are particular AI models trained on broad data that includes text, images, videos, and more. This technology is used for training Generative AI, which can perform a variety of tasks[33];

[29] LinkedIn, AI Talent in the European Labour Market, https://economicgraph.linkedin.com/content/dam/me/economicgraph/en-us/PDF/AI-TAlent-in-the-European-Labour-Market.pdf;

[30] See above;

[31] McKinsey & Company Leveraging generative AI in Europe: The opportunities and challenges, 13 October 2023, https://www.mckinsey.com/featured-insights/lifting-europes-ambition/leveraging-generative-ai-in-europe-the-opportunities-and-challenges#/ ;

[32] Francesco Di Ciommo, Camilla Scarpellino, Le priorità della Presidenza italiana del G7 sull'Intelligenza Artificiale, https://sog.luiss.it/policy-observatory/publications ;

[33] Zach Meyers, John Springford, How Europe can make the most of AI, https://www.cer.eu/publications/archive/policy-brief/2023/how-europe-can-make-most-ai ;

- since both Europe and the United States are currently working on developing guidelines to improve AI safety, security, and transparency, this is the right time to establish a common set of standards to enhance the development of trade relations between the two continents in the AI sector and facilitate the exchange of resources. This goal can be advanced through NGOs that gather stakeholders and researchers around draft standards. Indeed, any institution or private organization wishing to formulate effective and practical technical rules must be aware of the current state of the art, such as the best available security software, optimal test beds, or red-teaming practices. At present, this solution appears to be the quickest way to achieve a basic level of protection against discrimination and violations of rights in AI systems, as currently only big tech companies possess this information;
- AI technology presents a significant opportunity for addressing global and societal challenges. With this aim, the White House identified seven case studies in various scientific fields where AI can be harnessed for good: designing advanced semiconductors, discovering new materials, addressing climate change, revealing the fundamental physics of the universe, studying human behavior, organizations, and institutions, advancing fundamental understandings in the life sciences, and discovering new applications in this field[34].

[34] President's Council of Advisors on Science and Technology, REPORT TO THE PRESIDENT Supercharging Research: Harnessing Artificial Intelligence to Meet Global Challenge, April 2024, https://www.whitehouse.gov/wp-content/uploads/2024/04/AI-Report_Upload_29APRIL2024_SEND-2.pdf .