ARTIFICIAL INTELLIGENCE AS A LEGAL SUBJECT OR AS AN OBJECT TO LEGISLATE: THE PERSPECTIVE OF THE EUROPEAN LEGISLATOR

Vincenzo Ricciuto[1]

Abstract
Faced with the frequent threats of AI systems, the contribution clarifies the regulatory perspective adopted by the European Union in order to govern, in a complete and above all urgent manner, a phenomenon that has raised great fears, but also ambitious promises of economic development. In the view of the European legislator, and as emerges from the AIA, the product-risk approach would make it possible to prevent possible harmful applications of AI, making it increasingly safe, trustworthy, and ethical, in line with an anthropocentric vision of progress. On the opposite side are those who consider AI as the holder of rights and duties, as well as liable for the damage caused by it, since it is not just a question of compliance with certain standards, beyond which the guarantees that service providers must ensure increase. Now, the debate is still ongoing, yet an artificial person, to whom even personality rights can be attributed, is certainly not a surprising concept for law.

Keywords
Artificial Intelligence, European Union, AIA, Product-Risk Model, Personality Rights, Liability.

Summary

[1] Full Professor of Civil Law, Department of Law, Rome Tor Vergata University – Italy.

1. APPROACH AND SCOPE OF THE AI ACT (AIA)

The title of the draft *EU regulation on Artificial Intelligence*, the AIA, seems to imply that this AI regulation yearns to comprehensively and urgently regulate artificial intelligences. Such impression is further corroborated by the fact that the AIA is a rare case in which the EU directly regulated a subject matter with a regulation, that is the most invasive form of EU law harmonization.

In reality, the AIA will operate alongside a good number of other legal norms. Fundamentally, it adopts a risk-based approach, in order to prevent harmful applications of AI. In order to do so, it treats AI as a product and provides some safety rules[2]. The EU, however, is not merely aiming at AI safety, as it also strives to contribute to the creation of an ethical AI. Therefore, the *EU guidelines on ethics in artificial intelligence* and the *EU Guidelines for trustworthy AI* set up an ethical framework that adds up on the legal and technical layers of regulation provided by the AIA[3].

In a systematic perspective, the AIA clarifies the regulatory perspective on artificial intelligence. Theoretically, two alternative legislative approaches could be hypothesized. First, AI could be conceived as a subject, a legal person that can hold rights and take duties. Such an approach has long fascinated thinkers from different backgrounds, who question whether artificial intelligence could be compared with human intelligence[4]. A machine that mimics consciousness may take decisions, thus actively interacting in a bundle of conscious social relations. Consequently, it could autonomously be the subject in legal relations, cause torts, for which it could

---

[2] See. NOVELLI *et al.* 2023, 5, who argues that the AI Act was inspired by U.K. legislation on industrial product risks.

[3] See FLORIDI *et al.* 2022, 5. See also the *European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies* (2020/2012(INL)).

[4] See for a review of literature and cinematography on artificial consciousness, BUTTAZZO, 2001, 24.

be held liable, and, if taken to the most extreme consequences, even hold personality rights. An artificial persona is not, after all, a surprising concept in law. The debate on the attribution of personality rights to non-human subjects is ongoing[5], as if such fictitious entities were not to be relegated in the scope of monetary rights.

The second approach, which the European legislator opted for, is to conceive AI as an object. Understanding AI as a product on which third parties can hold rights implies that it qualifies as an asset, or in civil law terms, as a juridical good. The AIA aims at ensuring the security of AI as a standalone product and of other products that include AI technologies. When such products fail to achieve conformity to the standards set out by the AIA and its Annexes, the providers can be fined[6]. The fundamental issue of liability for damages that are caused by the AI is however targeted by another piece of legislation, which is the proposed *AI Liability Directive* (AILD). Here, the usage of a directive will enable Member States to reconcile EU objectives with national liability principles.

The AIA is in reality a partial provision, which creates a minimal legislative perimeter that defines the legal safeguards on AI, a phenomenon that raised fears, as well as the promise of economic development. Above all, the AIA introduces the first definition of artificial intelligence, albeit a very criticized one. The definition of AI it provides is quite generic, and it levers on the techniques used for training software that has the purpose of generating output such as content and recommendations. AI techniques include: machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; statistical

---

[5] For instance, also with regard to the attribution of copyright to AI powered machines, see WEI 2022.

[6] ZIOSI *et al.* 2023, 6.

approaches, Bayesian estimation, search and optimization methods. The definition is not included in the main body of the Regulation, but in its Annex I, in order to enable the EU Commission to promptly respond to emerging "AI threats". The fact that AI is defined in generic terms, such as "statistical approaches" is also due to the same reason, but could lead to uncertainty in its application.

On this backbone, future regulations will further construct, as is clarified by the AIA itself. AIA rules on AI conformity assessments clarify that the standards on which AI is evaluated can be twofold. AI that is offered as a standalone product will undergo AI-specific risk assessments[7]. On the other hand, AI that is incorporated in a product can be subject to industry specific assessments. On a separate note, several resolutions of the European Parliament foreshadow new legislation applicable to particular uses of AI, such as the impact of AI on copyright[8], criminal law[9], education, culture, and the audiovisual industry[10].

The uncertainty is even more relevant as the AIA is inspired by principles that are radically different to those that regulate the usage of online intermediary services that do not rely on AI. In fact, while the AIA adopts a product-risk approach and it prohibits certain AI practices, other legislations opt for different regulatory techniques.

The Digital Services Act (DSA) is, in many ways, complementary to the AIA. However, it does not adopt a product risk approach. On the contrary,

---

[7] In order to ensure that industry specific rules include AI related safety measures, the EU amended several industry standards, issuing a *Proposal for a Regulation of the European Parliament and of the Council on machinery products* and a *Proposal for a Regulation of the European Parliament and of the Council on general product safety*.

[8] *European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies* (2020/2015(INI)).

[9] *European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters* (2020/2016(INI)).

[10] *European Parliament resolution of 19 May 2021 on artificial intelligence in education, culture and the audiovisual sector* (2020/2017(INI)).

it treats hosting service providers and online platforms as intermediary service providers that are subject to set of liability exemptions, and other clauses, which are centered on their active role within the provision of online content. Because the DSA and AIA are mutual legislations, the fact that they adopt different criteria in determining both affected entities and legislative strategies could lead to legal uncertainty.

2. AIA OBJECTIVES

The objectives of the European Union in terms of AI development were coherently drawn out in the 2020 *White Paper on Artificial Intelligence: a European approach to excellence and trust*. They are expressly summarized in the AI Act, which singles out four main objectives: (1) ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values; (2) ensure legal certainty to facilitate investment and innovation in AI; (3) enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems; (4) facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation. The stress on fundamental rights, as well as the involvement of human surveillance in the security protocols laid out by the AIA, suggests that a goal of the EU is to promote an anthropocentric AI. This is also corroborated by the usage of terms such as human intervention and surveillance, technical robustness, security, privacy, data governance, transparency, diversity, non-discrimination, equity, social and environmental well-being, accountability. The numerous key terms laid out above refer to a combination of techniques that aim to ensure an anthropocentric AI:

1) Prevention principle: AI practices that may be detrimental to humans, such as those that rely on subliminal techniques, are prohibited. The same goes for AI practices that may be detrimental to certain categories of particularly vulnerable humans (for instance

because they could lead to the discrimination of certain ethnic or religious minorities), or that use some biometric tools that are in some circumstances deemed to be harmful.

2) A principles of control before market placement of AI products that are deemed to be high risk, through product tracking, security certificates and transparency duties towards consumers.
3) A principle of institutional cooperation, according to which not only Member States, but also competent supervisory and regulatory authorities should cooperate.

Some suggested however that four objectives are not equally important, as legal certainty to facilitate investments stands out over ethical principles[11]. Not only is legal consistency repeatedly mentioned in the *Memorandum*, but conflicts between different ethical principles are not solved, which, in turn, dilutes the overall importance of individual ethical principles[12].

There is also a further argument suggesting the prevalence of legal pragmatism over ethical concerns. The *Explanatory Memorandum of the AI Act Proposal*[13], promulgated by the European Commission reads such objectives in light of an underlying ambition of the EU to become a global leader in the development of secure, trustworthy and ethical artificial intelligence. Hence, the objectives laid out in the AIA should be interpreted in a way that does not "unduly constrain" or "hinder" technological development, not disproportionately increase the cost of placing AI products on the market[14].

---

[11] ANDERSON 2022, 3.

[12] FLORIDI cit., 72.

[13] par. 1.1.

[14] See also the whereas in addition to adjustments to existing legislation, legal and ethical questions relating to AI technologies should be addressed through an effective, comprehensive and future-proof regulatory framework of Union law reflecting the Union's principles and values as enshrined in the Treaties and the Charter of Fundamental Rights of the European Union ('Charter') that should refrain from over-regulation, by only closing existing legal loopholes, and increase legal certainty for businesses and citizens alike, namely

The aim to achieve global primacy in AI regulation could however be hampered by the very categories used by the AIA, that are typical categories of EU market regulation[15].

3. AIA PRODUCT-RISK MODEL

The draft IAI identifies some risk thresholds, above which the guarantees, that AI service providers must provide, increase. The highest level of risk (i.e., unacceptable risks) is listed in Art. 5. The norm enumerates AI "practices" that[16]: (a) deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behavior in a manner that causes or is likely to cause that person or another person physical or psychological harm; (b) exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behavior of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm; (c) if implemented by public agencies, classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score leading to: (i) unfavorable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected; (ii) unfavorable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social

by including mandatory measures to prevent practices that would undoubtedly undermine fundamental rights.

[15] See EDWARDS 2022.

[16] See ORLANDO 2022, 348, for a criticism of the expression "AI practices". The Author suggests that the AIA does not intend to qualify AI as an agent, but it really intends to say that people who use AI are prohibited from certain uses.

behavior or its gravity; (d) "real-time" remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for finding missing children or countering terrorist attacks.

With regard to the activities mentioned above, the AIA prohibits their placing on the market, putting into service and use of products described in article 5, a), b) and c); and the use of product described in article 5 d). The structure of the first three letters of the prohibition reinforces once again the impression that the AIA indeed treats AI as a software product[17].

Annex III indicates high-risk AIs, which are not prohibited, but must undergo a regime of compliance involving risk management, data-quality as well as the transparency of technical documents. The list is longer than that of Article 5, but all items can be referred to the following eight categories of AIs: critical infrastructures that could put the life and health of citizens at risk; AI systems intended to be used for biometric identification of natural persons; educational and vocational training, that may determine the access to the education and professional course of someone's life; employment, workers management and access to self-employment; essential private and public services; law enforcement systems that may interfere with people's fundamental rights; and migration, asylum and border control management; administration of justice and democratic processes. The EU Commission can add new subcategories, but it cannot introduce entirely new headings.

High risk AIs are at the core of the AIA, as their usage is not simply prohibited, but is subject to a complex legal regime. Entities that deploy AI systems will have to use the high-risk AI systems in accordance with the instructions of use, issued by the providers. On top of that, the AIA foreshadows the growth of sectorial legislation for the deployment high-risk AI systems in certain industries (e.g. a bank may have to comply with additional approval or control over a loan-system support AI system).

[17] Inthere, 351.

High risk AIs are also subject to a further set of duties, which aim at ensuring the quality of data they gather and use. In this sense, the AIA correlates with relevant provisions included in the GDPR. Systems classed as 'high-risk' must conform to the requirements in Chapter 2 of the AI Act. These broad requirements affect the development, deployment, and usage of a high-risk AI systems through their whole lifecycle. Importantly, Chapter 2 is not the only source of obligations relating to high-risk systems. But it sets out the "legal requirements for high-risk AI systems in relation to data and data governance, documentation and recording keeping, transparency and provision of information to users, human oversight, robustness, accuracy and security".

The requirements set out in Chapter 2 comprise a self- assessment for risks (art. 9), the quality and security of data (art. 10), the transparency of both technical standards and final outputs of the high-risk AI system (artt. 11-13), a principle of human oversight, and a principle of security[18].

Low risk AI systems are subject to mere transparency requirements, unlike minimal risk systems, such as those deployed in videogames.

[18] It is however still discussed whether algorithmic and AI explainability is possible at all, see THALPAGE 2023, 31-36.

REFERENCES

NOVELLI, Carlo *et al*, *How to Evaluate the Risks of Artificial Intelligence: A Proportionality-Based, Risk Model For The AI Act*, in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4464783, May 31, 2023.

FLORIDI, Luciano *et al.*, *Capai – A Procedure For Conducting Conformity Assessment Of AI Systems In Line With The EU Artificial Intelligence Act*, in *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4064091*, March 23, 2022.

BUTTAZZO, Giorgio, *Artificial consciousness: Utopia or real possibility?*, 24-30, in *Computer*, 34, 7/2001 (http://retis.sssup.it/~giorgio/paps/2001/ieeecm01.pdf).

WEI, Chenlin, *Copyright Protection and Data Reliability of AI-Written Literary Creations in Smart City*, in *Security and Communication Networks*, August 9, 2022.

ZIOSI, Marta *et al.*, *The EU AI Liability Directive: shifting the burden from proof to evidence*, in *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4470725, 2023*, June 6, 2023.

ANDERSON, Marc M., *Some Ethical Reflections on the EU AI Act*, in *CEUR Workshop Proceedings*, 3221, September 2022.

EDWARDS, Lilian, *Regulating AI in Europe: four problems and four solutions*, in https://www.adalovelaceinstitute.org/wp-content/uploads/2022/03/Expert-opinion-Lilian-Edwards-Regulating-AI-in-Europe.pdf, 2022.

ORLANDO, Salvatore, *Regole di immissione sul mercato e "pratiche di intelligenza artificiale" vietate nella proposta di Artificial Intelligence Act*, in *Persona e Mercato*, 3/2022.

THALPAGE, Nipuna S., *Unlocking the Black Box: Explainable Artificial Intelligence (XAI) for Trust and Transparency in AI Systems*, 31-36, in *Journal of Digital Art & Humanities*, 4, 1/2023.