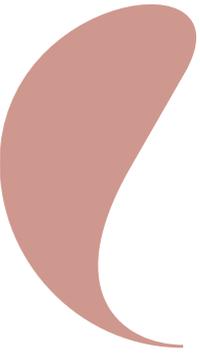
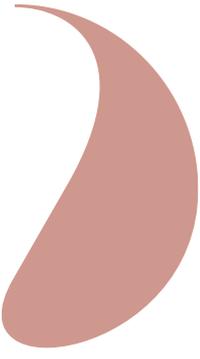


FEBRUARY 2023



FINE-TUNING THE AI ACT. DEFINITIONS, HIGH-RISK APPLICATIONS AND CONFORMITY ASSESSMENTS



Stefano da Empoli, Vincenzo Iaia

The policy brief is devoted to the Artificial Intelligence Act (AIA), which is the first (hard) law on AI by a major regulator anywhere. It aims at striking a balance between enhancing innovation while granting fundamental rights in the global race to unleash the potentials of AI. The underlying goal is to confirm European leadership as a global standard setter, as has already happened for the General Data Protection

- The analysis of the AIA starts from some key definitions set out in Art. 3. It appears that some of them - i.e., “in a view to”, “subliminal technique” (Art. 5.1.a) - need further clarification to avoid fragmented, and diverging, interpretations across Member States. If not, the attempt of a maximum harmonisation, which is endemic in European regulations, could be vain.
- The AIA is based on a risk-based approach. It provides a taxonomy of the activities carried out by AI with the corresponding legal regime, dividing them into three categories: (i) prohibited activities; (ii) high-risk activities; and (iii) low-risk activities. However, there are some doubts about the correct placement of certain activities in the corresponding cluster, especially regarding biometric identification systems.
- The proposal also raises further questions, namely, the treatment of general-purpose AI, the setting up of national and cross-border sandboxes, and the upskilling of regulators and companies.
- The AIA is without doubt an innovative piece of legislation that will play a crucial role in the European digital transition. Its effects would not only be restricted to the EU Member States, considering its consolidating role in setting global standards and exporting Union values.
- The main hope is that the regulation, once put in place, will still be consistent with the fast-changing technological reality.

1. THE TECHNICAL AND LEGAL FRAMEWORK UNDERLYING THE AI ACT

The ever increasing and pervasive interaction with Artificial Intelligence (AI) technologies in everyday life has drawn the attention of policymakers from all over the world to ensure that the multi-faceted applications of AI do not jeopardise fundamental rights in the global race for innovation.

AI is not a monolithic entity. The basic algorithmic approach used by AI is machine learning¹, which is a technique that uses data and algorithms to imitate the way humans learn. The system infers how to perform a task – or multiple tasks – making rules based on lots of examples. Through the extraction of data (or more often Big Data) by its self-learning algorithms, AI has the potential, for example, to improve healthcare, contribute to climate change mitigation and adaptation, improve the efficiency of production systems through predictive maintenance², produce new typically “intellectual” creations, such as writings³, music⁴, paintings⁵ and other forms of art⁶. As such, some new activities that (only) AI is able to perform raise questions on the protection of consumers and humans, in general.

The first EU intervention on AI dates back to 2018, when the Commission, after being invited by the European Council to put forward a “European approach to AI”⁷, presented the Communication “Artificial Intelligence for Europe”⁸. The Communication highlights the need to join public and private forces for the EU to become a leader in the AI revolution, allocating adequate resources to this promising technology and, at the same time, without sacrificing the Union’s values and fundamental rights.

¹ Deep learning and neural networks are sub-fields of machine learning characterised by the abstraction of human intervention. For an in-depth analysis of the technical processes governing them, see: E. ALPAYDIN, *Machine Learning*, The MIT Press, Cambridge (MA), 2021; H.C AGGARWAL, *Neural Networks and Deep Learning*, Springer, New York, 2018.

² EU Commission, White Paper ‘On Artificial Intelligence – A European approach to excellence and trust’, COM(2020)65 of 19 February 2020, 1.

³ See the press article drafted by the AI-system GPT-3 and published by The Guardian, *A robot wrote this entire article. Are you scared yet, human?*, London, 8 September 2020, available at the following link: <<https://www.theguardian.com/commentisfree/2020/sep/08/robot-wrote-this-article-gpt-3>>.

⁴ Listen the playlist ‘AI-composed music’ published on Spotify at the following link: at <<https://open.spotify.com/playlist/0qBf2Mqwb0GkrlliBhdvOU>>.

⁵ See the Rembrandt painting produced 350 years after his death at the following link: <<https://www.nextrembrandt.com/>>.

⁶ For a thorough research on the impressive capacity of AI to produce a wide variety of works in the *pantheon* of arts see: M. DU SAUTOY, *The creativity code. How AI is learning to write, paint and think*, HarperCollins, New York, 2019. For instance, streaming platform catalogues will soon be enriched with AI-produced movies. - Netflix has already released a horror-movie scripted by an AI, titled ‘Mr. Puzzles Wants You to Be Less Alive’. The AI ‘watched’ over 400,000 hours of horror movies enabling it to write its own. For further information, see: R. RUSAK, *Watch the first horror movie written exclusively by bots*, *Nerdist*, 7 October 2021, available at: <<https://nerdist.com/article/netflix-bot-written-horror-movie/>>. The awareness that AI can have an impact on the creative sector is also witnessed in the draft report on AI in a digital age (2020/2266(INI)) issued by the Special Committee on Artificial Intelligence on 2 November 2021, outlining that “In a Digital Age Artificial Intelligence (AI) determines the current digital transformation as the key technology. As a term encompassing a wide range of technologies that are guided by a given set of human-defined objectives and have some degree of autonomy in their actions, AI processes and responds to the data it receives, leading to learning, reasoning, planning, decision-making and creativity”. However, as argued in V. IAIA, *To Be, or Not to Be...Original Under Copyright Law, That Is (One of) the Main Questions Concerning AI-Produced Works*, in *GRUR International*, vol. 71, IX, 2022, pp. 793-812, this notion of creativity does not cover the special meaning that it assumes through the lens of copyright law, considering that AI is not capable of expressing the creative choices that make a work copyrightable.

⁷ European Council, *Cover note from General Secretariat of the Council to Delegations*, 19 October 2017, EUCO 14/17.

⁸ European Commission, *Communication Artificial Intelligence for Europe*, 25 April 2018, COM(2018) 237 final.

The Communication highlights the need to join public and private forces for the EU to become a leader in the AI revolution, allocating adequate resources to this promising technology and, at the same time, without sacrificing the Union's values and fundamental rights.

In June 2018, the Commission appointed the High-Level Expert Group on Artificial Intelligence (AI HLEG) to guide the upcoming legislative steps on AI. The AI HLEG worked closely with the European community of AI stakeholders through the AI Alliance, an online forum with over 4,000 members representing academia, business and industry, civil society, EU citizens and policymakers. The members of the AI Alliance offered detailed feedback for the “Ethics Guidelines for Trustworthy AI”⁹. Moreover, a set of materials such as policy documents, academic papers and discussions published on the forum, helped define the other deliverables of the AI HLEG¹⁰.

European institutions enacted many other soft laws dealing, directly or indirectly, with AI technologies, especially the Communication from the Commission “Shaping Europe’s Digital Future”¹¹ and its White Paper “Artificial Intelligence: a European Approach to excellence and trust”¹².

All these measures were the humus for the EU to present the AI package in April 2021. It encompasses the Communication on “Fostering a European Approach to Artificial Intelligence”¹³, a review of the “Coordinated Plan on Artificial Intelligence”¹⁴ and the proposal for a regulation laying down harmonised rules on AI (Artificial Intelligence Act or AIA)¹⁵. This document focuses on the AIA, the first (hard) law on AI by a major regulator anywhere. It aims at striking a balance between enhancing innovation while granting fundamental rights by adopting a risk-based approach (see infra par. 3) which, to some extent, echoes the European consumer protection rules¹⁶.

⁹ AI HLEG, *Ethics Guidelines for Trustworthy AI*, 8 April 2019, available at the following link: <https://www.aepd.es/sites/default/files/2019-12/ai-ethics-guidelines.pdf>.

¹⁰ The deliverables of the AI HLEG are available at the following link: https://digital--strategy-ec-europa.eu.translate.google/en/policies/expert-group-ai?_x_tr_sl=en&_x_tr_tl=it&_x_tr_hl=it&_x_tr_pto=sc

¹¹ European Commission, Communication *Shaping Europe’s Digital Future*, 2020, available at the following link: https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-digital-future-feb2020_en_4.pdf.

¹² European Commission, White Paper on Artificial Intelligence: a European Approach to Excellence and Trust, 19 February 2020, COM(2020) 65 final, available at the following link: https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

¹³ European Commission, Communication *Fostering a European Approach to Artificial Intelligence*, 21 April 2021, COM(2021) 205 final.

¹⁴ The review of the coordinated plan on AI is available at the following link: <https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review>.

¹⁵ European Commission, *proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts*, 21 April 2021, COM(2021) 206.

¹⁶ Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, L 328/7. The parallel of the two pieces of legislation has been stressed by M. ALMADA, N. PETIT, *The EU AI Act: Between Product Safety and Fundamental Rights*, 2022, available at SSRN at the following link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4308072.

The underlying goal is to confirm European leadership (at least) as a global standard setter¹⁷, as was the case for the General Data Protection Regulation¹⁸.

2. KEY DEFINITIONS

Starting in media res, Art. 3 of the AIA provides 44 definitions of the terminology used in the proposal with a view to preventing divergent interpretations across Member States. The first is dedicated to AI systems, seeking to end the numerous attempts to provide a perdurable definition of AI despite its constant evolution and its prismatic applications. This uncertainty is also witnessed at European level, as EU institutions have proposed several definitions, sometimes broader¹⁹, sometimes narrower²⁰. Indeed, from a pragmatic standpoint, it would be hard to reach a uniform consensus on the conditions that software should meet to be considered capable of simulating intelligence²¹.

Yet, EU institutions have presented definitions that, so far, struggle to completely capture the underlying technological processes or full capabilities of AI. For instance, the EU Parliament provided only a vague definition according to which: “An AI system means a system that is either software-based or embedded in hardware devices, and that displays behaviour simulating intelligence by, inter alia, collecting and processing data, analysing and interpreting its environment, and by taking action, with some degree of autonomy, to achieve specific goals”²².

Conversely, Art. 3(1) of the AIA borrows the definition provided by the US National Institute of Standards and Technology qualifying AI as 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”²³. This notion, focused on AI’s outputs –

¹⁷ Even if the Explanatory Memorandum of the AIA states that the proposal is aimed at preserving the EU’s technological leadership, it is well known that the major investments in AI are concentrated in the United States and in China, as stated in the report issued by the European Investment Bank, *Artificial intelligence, blockchain and the future. How disruptive technologies create opportunities for a green and digital economy*, Luxembourg, 2021. The report underlines that Europe needs to address an investment gap of up to € 10 billion that is holding back development and deployment of AI and blockchain technologies in the EU.

¹⁸ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, L 119/1.

¹⁹ See the Communication of the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Artificial intelligence for Europe*, COM(2018)237 of 25 April 2018, which stated that AI refers to “systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals”.

²⁰ See the precise definition drawn up by the AI HLEG, *A Definition of Artificial Intelligence: main capabilities and disciplines*, 18 December 2018, p. 6, which describes AI as “a complex of software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their actions”.

²¹ V. IAIA, *To Be, or Not to Be...Original Under Copyright Law, That Is (One of) the Main Questions Concerning AI-Produced Works*, cit., p. 794.

²² European Parliament, *resolution on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice*, of 20 January 2021, 2020/2013(INI), para 1.

²³ Art 3(1) of the proposal for the AIA. Annex I contains the following techniques: “(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;

aside from the critics highlighting the danger of anthropomorphism that arise from the terms Artificial Intelligence per se²⁴ –, seems more persuasive than the others provided by the EU institutions because it places emphasis on the human origin of the settings, which is a key aspect for allocating responsibilities.

However, some notions appear less straightforward. For instance, Art. 3(2) qualifies the provider as a “natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge” (emphasis added). Drawing legal consequences from mere intentions, which can be confined to unfulfilled wishes, risks producing arbitrary effects, setting aside the related diabolical burden of proof. This is also bolstered by the fact that researchers are not always able to foresee the potential downstream uses of their outcomes, and even if there is a product/service idea underpinning development, the final version will often differ substantially from its original vision.

Hence, the language “with a view to” to define a “provider” of AI would create legal uncertainty about which operators fall into the scope of the provision, risking to discourage researchers from making progress in this promising domain. It would seem preferable to adopt a more pragmatic approach that qualifies as providers – with the related obligations of conformity assessments (see infra par. 3) – only those operators that (effectively) place on the market or put into service an AI system.

Moreover, Art. 5, which lists the banned AI practices, prohibits, in par. (1)(a), “the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person’s consciousness in order to materially distort a person’s behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm”. There are conduct and features that may influence, more or less subtly, the user’s behaviour, such as accepting a less protective privacy policy²⁵. For example, the simple practice of product placement in TV shows can tacitly affect an individual’s attitude²⁶. Here, Recital 16 of the AIA specifies that some AI systems “deploy subliminal components individuals cannot perceive or exploit vulnerabilities of children and people due to their age, physical or mental incapacities. [...] Research for legitimate purposes in relation to such AI systems should not be stifled by the prohibition, if such research does not amount to use of the AI system in human-machine relations that exposes natural persons to harm and such research is carried out in accordance with recognised ethical standard for scientific research”. Further illustrations would be useful to better distinguish the lawful from unlawful activities since the current understanding of “materially distorting” or “subliminal techniques” may give rise to blurry areas.

(b) Logic and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; (c) Statistical approaches, Bayesian estimation, search and optimization methods’. It follows Recital 6 of the Act, which outlines that ‘The notion of an AI system should be clearly defined to ensure legal certainty, while providing the flexibility to accommodate future technological developments. [...] The definition of an AI system should be complemented by a list of specific techniques and approaches used for its development, which should be kept up-to-date in the light of market and technological developments through the adoption of delegated acts by the Commission to amend that list’.

²⁴ G. FINOCCHIARO, *La regolazione dell’intelligenza artificiale*, in *Rivista Trimestrale di Diritto Pubblico*, IV, 2022, 1087.

²⁵ See, for instance, the effects of the automatic implementation of Android applications, M. DI, S. NAZIR, F. DENG, *Influencing User’s Behavior Concerning Android Privacy Policy: An Overview*, in *Mobile Information System*, 2021.

²⁶ L. CHEE KIT, E. LIM QUI P’NG, *The Effectiveness of Product Placement: The Influence of Product Placement towards Consumer Behavior of the Millennial Generation*, in *International Journal of Social Science and Humanity*, vol. 4, II, 2014, pp. 138-142.

This gap may be filled by borrowing the definition of the practice “to materially distort the economic behaviour of consumers” set out by Art. 2, let. E) of the Unfair Commercial Practices Directive, qualifying it as “using a commercial practice to appreciably impair the consumer’s ability to make an informed decision, thereby causing the consumer to take a transactional decision that he would not have taken”. This assessment should be based from the perspective of the average member of the group of consumers targeted by this practice²⁷. However, there is a fine line between persuasion (lawful) and aggressive intrusion (unlawful) which cannot but be drawn by courts on a case-by-case approach.

There is a fine line between persuasion (lawful) and aggressive intrusion (unlawful) which cannot but be drawn by courts on a case-by-case approach.

3. THE RISK-BASED TAXONOMY OF AI ACTIVITIES

As mentioned above, the AIA entails a risk-based approach. It provides a taxonomy of the activities carried out by AI depending on their likelihood to endanger fundamental rights. AI practices are divided into three categories: (i) prohibited activities; (ii) high-risk activities; and (iii) low-risk activities. Tailored rules correspond to each cluster.

Firstly, Art. 5 covers the banned activities (i.e., social scoring), referring to the placing on the market, putting into service or use of an AI system that:

1. deploys subliminal techniques beyond a person’s consciousness in order to materially distort a person’s behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm;
2. 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 behaviour of a person pertaining to that group or in a manner that causes or is likely to cause that person or another person physical or psychological harm;
3. evaluates or classifies, for public authorities or on their behalf, the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics;
4. uses “real-time” remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless it fulfils security purposes or law enforcement.

A lively debate has concerned the classification of real-time biometric identification systems in the prohibited practices. Some parties would prefer an outright ban with no exceptions because of their intrusiveness, while, on the other hand, many governments would like to maintain a full access to biometric technologies for security purposes. In the amendments recently shared by the co-rapporteurs on the AIA, the use of biometric traits to categorise people using or inferring sensitive or protected attributes falls within the prohibited practices²⁸. They also express the willingness to ban AI models that fill in facial recognition databases by indiscriminately scrapping face images from social media pictures and any

²⁷ CJEU, judgement of 12 June 2019, Case C-628-17, *Polska*, ECLI:EU:C:2019:480.

²⁸ L. BERTUZZI, *AI Act: All the open political questions in the European Parliament*, Euractiv, 13 February 2023, available at the link: <https://www.euractiv.com/section/artificial-intelligence/news/ai-act-all-the-open-political-questions-in-the-european-parliament/>.

other use cases listed under the list of high-risk area²⁹. In any case, the ban does not concern one-to-one recognition systems to check the identity of the user for specific services (i.e., accessing one's home or office building).

According to Art. 6, an AI system is considered high-risk when both the following conditions are met:

1. the AI system is intended to be used as a safety component of a product, or is itself a product;
2. the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product.

The high-risk activities are listed in Annex III of the AIA and include, for instance, CV-scanning tools that rank job applicants. Those practices are subject to specific legal requirements, in terms of risk management systems (Art. 9), data governance (Art. 10), technical documentation (Art. 11), record-keeping (Art. 12), transparency obligations (Art. 13), human oversight (Art. 14), accuracy, robustness and cybersecurity (Art. 15). According to Art. 7, the Commission has the power to update the list in Annex III by adding new high-risk AI systems that may cause a harm to health, safety, or fundamental rights.

In this perspective, businesses should constantly monitor Annex III to follow its updating in order to ensure compliance with the AIA. The EU should facilitate the communication with interested businesses through a newsletter covering the amendments. It should also consider obligations based on the size of the companies offering high-risk AI applications since big companies can afford the high costs for obtaining the required certifications, while small and medium enterprises may find them disproportionate compared to their revenues³⁰.

One controversial aspect concerns data governance, since Art. 10(3) states that “training, validation and testing data sets shall be relevant, representative, free of errors and complete”.

One controversial aspect concerns data governance, since Art. 10(3) states that “training, validation and testing data sets shall be relevant, representative, free of errors and complete”. This provision does not seem to reflect the practical reality...

This provision does not seem to reflect the practical reality because real-world data sets will almost never be free of errors, especially considering that Big Data is made up of millions or billions of individual points. It is also unclear how to measure the relevance and representativeness of such data sets, as different metrics are available. Moreover, it is hard to affirm the completeness of a data set because there will always be space for its updating. However, at some point, it should be considered good enough. Hence, policymakers may evaluate a softening of the obligation by rephrasing the article to require AI providers to ensure that training, validation and testing data sets would be conducted according to industry best practices. This would make the obligation more feasible while encouraging the best efforts of developers to ensure data correctness.

Thirdly, Art. 52 provides transparency obligations for some low-risk AI practices. The disclosure requirement applies to AI systems that (i) interact with humans; (ii) are used to

²⁹ *Ibidem*.

³⁰ G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale*, cit., 1096.

detect emotions or determine association with (social) categories based on biometric data; (iii) generate or manipulate content (“deep fakes”).

Moreover, there is a current debate on which cluster best fits general-purpose AI systems. These systems allow the deployers to apply them in myriads of ways, with a wide range of potential benefits and risks³¹. For instance, Chat GPT (Generative Pre-trained Transformer), the chatbot produced by OpenAI that has recently become popular for its quick tailored (though often incorrect) answers, qualifies as a general-purpose AI system. The classification of general-purpose AI as high-risk application may hinder the development of this promising technology because of the conformity assessments and the other strict obligations established by Arts. 9-15 of the AIA, even when the system does not perform high-risk activities.

The allocation of responsibilities between the provider and the deployer of the general-AI should be based on which actor is the best positioned to understand which controls and risk mitigations are most appropriate to the specific use of the AI and implement them appropriately. The distribution of responsibilities along the value chain of general-purpose AI is expected to be a hot topic of discussion during trilogue meetings³².

Another issue is the upskilling challenge in a highly technical field, both on the sides of regulators and companies. The EU and its Member States should promote media literacy for sharing knowledge of AI among undertakings (especially SMEs) and the public at large. At the same time, AI providers and deployers should enhance digital skills by providing AI literacy for their staff, including practical explanations to comply with the AIA.

The classification of general-purpose AI as high-risk application may hinder the development of this promising technology because of the conformity assessments and the other strict obligations established by Arts. 9-15 of the AIA, even when the system does not perform high-risk activities

Finally, the Parliament foresees the obligation for each EU country to set up at least one regulatory sandbox, a controlled environment where AI technology could be tested, and is envisioning the possibility for Member States to establish it jointly with other countries.

³¹ The reference in the definition of AI system that the software is based on a given set of objectives could not be compatible with general-purpose AI since it can be adapted to carry out a wide range of tasks. However, as reported by L. BERTUZZI, *AI Act: All the open political questions in the European Parliament*, cit., the European Parliament’s rapporteurs on the AI Act Brando Benifei and Dragos Tudorache made it explicit that this “reference [...] is not related to the final goal or purpose of the system, but rather to the parameter optimisation process within the model. Such objectives may be both explicit and implicit”.

³² If general-purpose qualifies as high-risk activity, its legal framework will be complemented by the final version of the proposal for a EU and Council directive on adapting non-contractual civil liability rules to AI (AI Liability Directive), 28 Sept. 2022, COM(2022) 496 final. The scope of the proposal is limited to the non-contractual fault-based civil liability caused by high-risk AI systems. Its objective is to modernise the EU liability framework to ensure that persons harmed by AI enjoy the same level of protection as persons harmed by other technologies. In its current version, Art. 4 of the proposal introduces a rebuttable presumption of a causal link between the fault of the defendant and the output produced by the AI system (or the failure of the AI system to produce an output) to ease the burden of proof for victims of this technology.

According to a recent compromise text, presented by the co-rapporteurs³³, the public authority establishing the sandbox would have to deliver to the AI Office and the European Commission an annual report to be published together with all the relevant information on a website to be managed by the EU executive. The Commission should be tasked with adopting a delegated act to define how sandboxes should be established and supervised within one year from the regulation's entry into force.

³³ L. BERTUZZI, *AI Act: co-rapporteurs seek closing high-risk classification, sandboxes*, Euractiv, 26 January 2022, <https://www.euractiv.com/section/artificial-intelligence/news/ai-act-co-rapporteurs-seek-closing-high-risk-classification-sandboxes/>