Walter Hallstein Institut
für Europäisches Verfassungsrecht
Humboldt-Universität zu Berlin

WHI-Paper 01/2023

The European Artificial Intelligence Act – remaining challenges for the legislature in the trilogue[1]

Kalojan Hoffmeister

[1] The manuscript was completed in August 2023. Subsequent developments are not taken into account.

A. Introduction

There is little doubt that artificial intelligence (AI) will be the next disruptive technology heavily impacting society and democracy. In April 2021, the European Commission proposed an Artificial Intelligence Act (henceforth COM-AIA) with the objective too address threats to the security of citizens, challenges to EU fundamental rights and values, the legal uncertainty arising from this new technology and general societal mistrust towards AI. The Brussels executive also wishes to pre-empt a potential fragmentation of the EU internal market and strengthen the digital sovereignty of the Union. Meanwhile both the Council of the European Union and the European Parliament have defined their positions on the Commission's proposal (henceforth Council-AIA and EP-AIA respectively). The trilogues are about to begin.

The aim of this paper is to provide a holistic overview of the most prominent open questions the AI text poses to the legislature.

After tracing the historical path towards the proposed AI-Act (B.) it examines the European Commission's proposal in detail considering the positions of the co-legislator (C.) before drawing a conclusion (D.).

B. The road to a European regulatory framework for AI

The idea of an AI regulatory framework in Europe is relatively young. The Commission only published its first thoughts on regulating AI in a Communication in April 2018.[2] It also established a "High Level Expert Group on AI" which published ethical guidelines

[2] Communication From The Commission To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions Artificial Intelligence for Europe 2018. (COM 2018(yyy) final).

for trustworthy AI[3] and policy and investment recommendations a year later[4] . In December 2018, the European executive presented a Coordinated Plan for AI.[5] This was followed by a further Communication[6] (2019) and an Expert Group Assessment List.[7] The White Paper of February 2020[8] stimulated a broad multi-stakeholder discussion, the outcome of which was published in an advisory paper. But the European Council, the Council and the European Parliament (EP) were not idle either: In 2017[9], 2019[10] and 2020[11] respectively, the European Council and the Council stressed the urgency of the issue and the importance of fundamental rights protection in the light of AI. The EP, in turn, called on the Commission to take legislative action in the field of AI as early as 2017 in a robotics resolution[12] . The House adopted another resolution in June 2020 on AI and industrial policy[13] and finally set up its own special committee on AI in June 2020.[14] This was followed by a series of resolutions in October 2020 on ethics[15] , liability[16] and copyright.[17] Further resolutions in the area of law enforcement,[18] education, culture and audio-visual[19] came along. In May 2022, the Parliament published a comprehensive resolution[20] consol-

[3] 'Ethics Guidelines for Trustworthy AI | Shaping Europe's Digital Future' (8 April 2019) <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> accessed 18 April 2023.
[4] 'Policy and Investment Recommendations for Trustworthy Artificial Intelligence | Shaping Europe's Digital Future' (26 June 2019) <https://digital-strategy.ec.europa.eu/en/library/policy-and-investment-recommendations-trustworthy-artificial-intelligence> accessed 18 April 2023.
[5] 'Coordinated Plan on Artificial Intelligence | Shaping Europe's Digital Future' (7 December 2018) <https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence> accessed 18 April 2023.
[6] 'Communication: Building Trust in Human Centric Artificial Intelligence | Shaping Europe's Digital Future' (8 April 2019) <https://digital-strategy.ec.europa.eu/en/library/communication-building-trust-human-centric-artificial-intelligence> accessed 18 April 2023.
[7] 'Assessment List for Trustworthy Artificial Intelligence (ALTAI) for Self-Assessment | Shaping Europe's Digital Future' (17 July 2020) <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment> accessed 18 April 2023.
[8] 'White Paper on Artificial Intelligence: A European Approach to Excellence and Trust' <https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en> accessed 18 April 2023.
[9] 'European Council Conclusions, 19/10/2017' 8 <https://www.consilium.europa.eu/en/press/press-releases/2017/10/20/euco-conclusions-final/> accessed 18 April 2023.
[10] Council of the European Union, AIb) Conclusions on the coordinated plan on ai adoption
[11] European Council, Special meeting of the European Council - Conclusions EUCO 13/20, 2020.
[12] European Parliament resolution 2015/2103(INL).
[13] European Parliament resolution 2018/2088(INI).
[14] European Parliament decision 2020/2684(RSO).
[15] European Parliament resolution 2020/2012(INL).
[16] European Parliament 2020/2014(INL).
[17] European Parliament resolution 2020/2015(INI).
[18] European Parliament Draft Report, 2020/2016(INI).
[19] European Parliament Draft Report 2020/2017(INI).
[20] European Parliament resolution, 3th May 2022, P9_TA(2022)0140.

idating its position on AI issues. It should be recalled, however, that the Council's conclusions and the Parliament's resolutions have no legal effect. This is because only the Commission has the right of initiative for binding legislation within the framework of the Treaties according to Art. 17 TEU.

The Commission published its "Proposal for a Regulation laying down harmonised rules on artificial intelligence", in short: Artificial Intelligence Act (AIA), on 21 April 2021. The European Economic and Social Committee[21], the European Committee of the Regions[22], the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS)[23] and the European Central Bank (ECB)[24] delivered their opinion in the second half of 2021.

The co-legislators are, however, only the Parliament and the Council. Consultations in the Council started under the Portuguese Presidency (first half of 2021), continued with the Slovenian (second half of 2021) and French Presidency (first half of 2022). The Council eventually adopted a general approach to the AIA during one of the last meetings of the Czech presidency in December 2022. In the European Parliament, the discussions are led by the Committee on Internal Market and Consumer Protection and the Committee on Civil Liberties, Justice and Home under a joint committee procedure. The Legal Affairs Committee (JURI), the Committee on Industry, Research and Energy (ITRE) and the Committee on Culture and Education (CULT) are associated to the legislative work with shared and/or exclusive competences. The Parliament adopted its general approach to the AIA in mid-June 2023. Thereafter the trilogues are set to begin.

C. The Commission's draft Artificial Intelligence Act (COM-AIA)

[21] 'EESC Opinion on the Artificial Intelligence Act' (*European Economic and Social Committee*, 26 March 2021) <https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/regulation-artificial-intelligence> accessed 16 April 2023.

[22] 'Opinion of the European Committee of the Regions — European Approach to Artificial Intelligence — Artificial Intelligence Act (Revised Opinion)' <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021AR2682#:~:text=High%2Drisk%20AI%20systems%20should,market%20or%20putting%20into%20service.>.

[23] 'EDPB-EDPS Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) | European Data Protection Board' <https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en> accessed 16 April 2023.

[24] Opinion of the European Central Bank of 29 December 2021 on a proposal for a regulation laying down harmonised rules on artificial intelligence (CON/2021/40) 2022/C 115/05 2021.

I. Defining AI and the scope of application of the Regulation

Any attempt to regulate dynamic and constantly evolving technologies inevitably encounters two fundamental challenges from the start: a) How can the technology in question be defined? And b) how broad should the scope of application of the regulatory framework be without jeopardising innovation and technological progress?

1. Definition of Artificial Intelligence, Art. 3 AIA in conjunction with Annex I

In the case of AI, defining the technology proves particularly difficult. A universally agreed definition of AI does not exist. *Hacker*[25] prefers - with reference to *Mitchell*[26] - to speak of *machine learning regulation* instead of AI. *Nemitz/Pfeffer*[27] also equate the terms artificial intelligence and machine learning and understand them to mean "the ability to solve difficult problems as independently as possible, i.e. without clear specifications"[28] , in other words “autonomously”. However, the concept of "autonomy" also poses difficult problems of delimitation. One of the primary difficulties with the concept of autonomy in AI is determining the degree to which an AI system is actually autonomous. Currently no widely accepted methodology exists for assessing autonomy in AI.

Art. 3 (1) of the COM-AIA avoids these problems by proposing the following definition:

> *"artificial intelligence system" (AI system) means 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 Commission thus chooses an enumerative approach, combined with elements of a human given goal that is met with generated outputs. Furthermore, the Commission empowers itself by giving itself the possibility to

> *“to amend the list of techniques and approaches listed in Annex I, in order to update that list to market and technological developments on the basis of characteristics that are similar to the techniques and approaches listed therein.“* (Art. 4)

[25] Philipp Hacker, ‘AI Regulation in Europe’ [2020] SSRN Electronic Journal 3 <https://www.ssrn.com/abstract=3556532> accessed 11 April 2023.
[26] Tom M Mitchell, *Machine Learning* (McGraw-Hill 1997) 2.
[27] Paul Nemitz, *Prinzip Mensch: Macht, Freiheit Und Demokratie Im Zeitalter Der Künstlichen Intelligenz* (Dietz 2020).
[28] ibid 44.

Hence, the Commission would have very wide discretional powers to define what AI means, as it would become the only competent body empowered to update Annex I which defines what AI is considered to be under the regulation. The chosen definition by the Commission has repeatedly been criticized as being too broad and bringing potential harm to the investment and development of the EU's AI market.[29]

The Council, on the other hand proposed in its general approach[30] (Council-AIA) a narrower definition and brings the notion of autonomy back to the table. The text reads

> "*'artificial intelligence system' (AI system) means a system that is designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts".*

This definition, although at first sight similar to the one provided by the Commission, is narrower. It is restricted to machine learning and logic- and knowledge based approaches, whereas Annex I which is used in the COM-AIA also includes "Statistical approaches, Bayesian estimation, search and optimization methods" and can be expanded. The Council also deletes the Commission's powers to add new systems through amending Annex I (Art. 4). Instead, it limits the Commissions powers to adopting implementing acts to further specify and update techniques under machine learning approaches and logic- and knowledge-based. Specifying already considered techniques is not the same as updating the list of (new) techniques.

The European Parliament for its part seems to have settled on the OECD definition of AI.[31] The text reads:

---

[29] see just the recently published opinion by Patrick Grady, 'The AI Act Should Be Technology-Neutral', n.d.

[30] Council General approach - 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 2022.

[31] Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts [(COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))1]; Luca Bertuzzi, 'EU Lawmakers Set to Settle on OECD Definition for Artificial Intelligence' (*www.euractiv.com*, 7 March 2023) <https://www.euractiv.com/section/artificial-intelligence/news/eu-lawmakers-set-to-settle-on-oecd-definition-for-artificial-intelligence/> accessed 12 April 2023.

> *"Artificial intelligence system' (AI system) means a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate output such as predictions, recommendations, or decisions influencing physical or virtual environments".*

As we can see, it is difficult to define what AI really is, especially as it is central to the regulation. Keeping it broad could on the one hand ensure that as many AI programmes as possible are covered. On the other hand, a great number of companies would be affected by the requirements of the AIA, which in turn could lead to considerable financial burdens and possibly hamper investment and innovation.
A narrower scope of application for its part could provide more legal certainty. Especially, if, as the Council proposes, the Commission were empowered by implementing act to define more precisely what is meant by "machine learning approaches and logic- and knowledge-based", then companies and AI developers would know better whether they fall under the AIA or not. It would make it clearer if the law applies to them or not. This would be a welcome development, as manageable criteria would lead to more predictability and avoid difficult-to-predict case-by-case casuistry. Yet, a narrow scope of application would run the risk of opening loopholes. The question surrounding the definition of AI is a typical example of the balancing act between the desire for the greatest possible legal protection through broad and flexible handling of the scope of application on the one hand, and the desire for legal certainty through terms that are as concrete and narrow as possible on the other. Ultimately, this constitutes a political choice.

2. Questions surrounding the scope of application, Art. 2 AIA

As for the scope of application of the regulation, the COM-AIA poses two questions: First, what is to be understood by "output…used in the Union"., and, second, whether scientific research is covered.

a) What does „output … used in the Union" mean? , Art. 2 AIA

According to Art. 2 COM-AIA the regulation applies not only to providers who place their product on the internal market, whether they are established in the Union or not (Art. 2 (1) lit. a), to AI users in the Union (Art. 2 (1) lit.b), but also to *"providers and users of*

AI systems that are located in a third country, where the output produced by the system is used in the Union;" (Art. 2 1 lit.c). But what does the wording mean that the *"output [...]is used in the Union"? Palka* rightly asks whether the regulation already applies when the product is made available to European users or only when one of them decides to use it?[32] Parliament tries to provide some more precision on this question: *„(c) providers and deployers of AI systems that have their place of establishment or who are located in a third country, where either Member State law applies by virtue of a public international law or the output produced by the system is intended to be used in the Union;"* (Art. 2 (1) lit. e EP-AIA).

But even with this, there is hardly a constellation conceivable in which AI applications encounter the European internal market without the Regulation applying. Hence, it seems reasonable to assume that due to the broad scope of application - similar to the GDPR - the so-called "Brussels effect"[33] could occur.

b) The question of scientific research

The next question arises as to whether scientific research also falls within the scope of the regulation.[34] Let's clarify the situation again: According to Art. 2 (1) (a) COM-AIA, the regulation applies to "providers who place AI systems on the market or put them into operation in the Union [...]". A "provider" in this sense is, according to Art. 3 (2), "a natural or legal person, public authority, agency or other body that develops an AI system or has it developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for consideration or not". According to Art. 3 (11), "putting into service" is "the making available of an AI system on the Union market for initial use directly to the user or for own use in accordance with its intended purpose". A scientific research institution is usually not a supplier that develops a product in order to make it available on the Union market for direct first use in return for payment. However,

[32] Przemyslaw Palka, 'The Phantom Menace: A Critique of the European Commission's Artificial Intelligence Act Proposal, Przemyslaw Palka' 9 <https://law.yale.edu/yls-today/yale-law-school-events/phantom-menace-critique-european-commissions-artificial-intelligence-act-proposal-przemyslaw-palka> accessed 12 April 2023.

[33] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (1st edn, Oxford University Press 2020) <https://academic.oup.com/book/36491> accessed 12 April 2023.

[34] Nathalie A Smuha and others, 'How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act' [2021] SSRN Electronic Journal 15, 16 <https://www.ssrn.com/abstract=3899991> accessed 12 April 2023.

a research institution could fall under the definition of a supplier that provides an AI system 'free of charge' for 'own use according to its intended purpose'. Accordingly, such scientific research institutions would become a provider under the regulation. Consequently though, this triggers a multitude of obligations. Especially, if the scientific AI-system is considered a high-risk system (see below). Being faced with the regulatory obligations of the AIA could lead to increased bureaucracy, higher compliance costs, and thus fewer resources allocated to research and scientific progress. As for the initial AIA, the text is ambivalent in this regard. On the one hand recital 16 COM-AIA states that "[research] for legitimate purposes related to such AI systems should not be suppressed by the prohibition if such research does not amount to use of the AI system in human-machine relationships that harm natural persons and if such research is conducted in accordance with recognised ethical standards for scientific research." On the other hand, an exception for scientific research has not been included in the operating part of Art. 5 on prohibited AI-systems.

The Council seems to have identified this problem and proposes that the AIA "*shall not apply to AI systems, including their output, specifically developed, and put into service for the sole purpose of scientific research and development. This Regulation shall not apply to any research and development activity regarding AI systems"* (Art. 2 (3) Council-AIA).[35]

Similarly, Parliament has also put forward an exception for *"to research, testing and development activities"* provided "*that these activities are conducted respecting fundamental rights and the applicable Union law"* (Art. 2 (5) d EP-AIA Overall, there seems to be consensus that research and development shall be excluded from most legal requirements of the AIA. Yet, it remains unclear how a fundamental rights "check" as requested by Parliament can be ensured.

II. Risk-based approach

[35] Council General approach - 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 (n 29) art 2 (6) and (7) respectively.

A key characteristic of the AI Act is its risk-based approach. Like the General Data Protection Regulation[36] (Art. 32-35 GDPR) the AIA defines risk categories that require different levels of compliance. Three levels are defined: unacceptable risk, high-risk and low or minimal risks.

1. Unacceptable risk - prohibited AI applications (Title II)

Title II of the AIA devotes its sole Art. 5 to prohibited AI applications. In an enumerative manner, manipulative systems causing harm, social scoring and real-time remote biometric systems are prohibited.

a) Introducing a possibility to add new technologies to the prohibited AI practices – a new Art. 5a AIA?

As a preliminary note, it should be pointed out that the COM-AIA does not provide for any possibility to amend the list of prohibited AI systems. In other words, the European legislator is stuck with those few prohibited AI-applications it now agrees on, unless it decides to change the legal text through a complex and time-consuming legislative process. Of course, such a rigid system provides for legal certainty. But considering the fast-changing technological developments and potential detrimental risks for fundamental rights and European democracy one can question whether such an inflexibility is wise. Further, the enumerated AI applications listed in Art. 5 will probably be the result of political compromise and horse trading. Against this background it might be desirable to open up the possibility to update the prohibited AI practices through delegated acts. Of course, a prohibition is the strongest possible intervention on the developers and companies fundamental rights, such as the freedom of business and right to property. Hence, such prohibition acts must in turn respect high standards and a set of clear and demanding criteria.

b) Manipulation, Art. 5 lit. a) and b) AIA

The COM-AIA prohibits AI-systems (1.) that manipulate persons subliminally and beyond their awareness (Art. 5 lit.a), (2.) that manipulatively influence a vulnerable group

[36] 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 (General Data Protection Regulation.

of persons due to age, physical or mental disability (Art. 5 lit.b) and can thus cause physical or psychological harm to this or another group of persons. In this respect, it is often referred to as surveillance capitalism, “informational capitalism”, “hypernudge”, “deception by design”, “erosion of autonomy” or “behavioral modification machines*”*.[37] At first glance, this is an important and correct regulatory starting point. However - as *Hacker* rightly recognises[38] - a precise reading of the wording does not seem unproblematic. Art. 5 (1) lit. a) and recital 16 COM-AIA, for example, imply a certain purposefulness with the wording *"in order to".* But, targeted manipulation will only be proven in very few cases[39] leading to less legal protection against manipulation than hoped for. Furthermore, the meaning "physical and mental disability" is unclear. Also, the chosen terms such as "subliminal influence" and exploitation of "weakness or need for protection" are not classic legal terms. How these will be interpreted by administration and courts raises a big question mark. Guidance is badly needed.

The criticism of these vague notions becomes even more seriouswhen one considers the following example, given by *Palka*[40] *:* The algorithms behind Facebook's newsfeed, Amazon's pricing, YouTube's recommendation videos and Google's advertising are known to wield[41] great power - including political power[42] . Social media addiction is also a serious problem and has a negative impact on the concentration and attention span of users. If one were now to assume that damage to attention span is "psychological damage" within the meaning of Art. 5 (1) lit. (b) AIA, this would lead to the result that Facebook, Google, Amazon and other advertising algorithms would be unlawful under the new AIA. It is highly doubtful whether this is the aim of the AIA.

Therefore, both Council and Parliament have amended the wording to “with the objective to or the effect of materially distorting a person’s behaviour […]”. Parliament added one exception to the manipulation prohibition though: The prohibition of AI system that de-

[37] Przemyslaw Palka, ‘The Phantom Menace: A Critique of the European Commission’s Artificial Intelligence Act Proposal, Przemyslaw Palka’, 4 with numerous further references, accessed 12 April 2023, https://law.yale.edu/yls-today/yale-law-school-events/phantom-menace-critique-european-commissions-artificial-intelligence-act-proposal-przemyslaw-palka.

[38] Philipp Hacker, ‘Manipulation by Algorithms. Exploring the Triangle of Unfair Commercial Practice, Data Protection, and Privacy Law’ [2021] European Law Journal eulj.12389, 31.

[39] ibid.

[40] Przemyslaw Palka (n 31) 10.

[41] ibid.

[42] Katarina Kertysova, ‘Artificial Intelligence and Disinformation: How AI Changes the Way Disinformation Is Produced, Disseminated, and Can Be Countered’ (2018) 29 Security and Human Rights 55.

ploys subliminal techniques shall not apply to AI systems intended to be used for approved therapeutical purposes. In any case, this overseen loophole now seems to have been dealt with.

c) Social scoring, Art. 5 lit. c) AIA – trustworthiness, private social scoring, time-period and conditionality questions

Art. 5 lit. c prohibits the so-called "social scoring" or social point system. This provision seems to be inspired by a wish to prevent a “Chinese-style” social credit system which introduces “punishments” such as travel bans, school bans, reduced employment prospects and even public shaming for individuals and companies which do not comply with the set expectations.[43]

Although the intention of the prohibition is a good one, there remain still some fallacies in the Commission’s proposal. For starters, it is unclear what "trustworthiness of the person" means. Then, it is noteworthy what is not in the AIA: The Commission’s proposal only refers to public authorities or actors acting on their behalf. Private systems are not included. Why a distinction is made between state and private actors is not apparent. Especially when one considers that in today's world there are certainly private economic actors who have an important, almost state-like position in society. This is ever more true when referring to essential public goods and services that have been privatised over the years (Deutsche Telekom, Deutsche Post, Frankfurt Airport, Orange [formally France Telecom], Electricité de France, Gaz de France, French highways, parts of the Spanish national rail, Spanish energy companies such as Endesa and Iberdola, Polish airline LOT etc.). This shortcoming was also identified by the Council and Parliament. In their general approach the explicit reference to public authorities is deleted, thus removing the implicit distinction between public and private actors.

Additionally, as *Raposo* argues[44], the required time frame “over a certain period of time” might exclude “episodic scoring”. Generally, evaluating something “over a certain period of time”, implies looking at the overall performance or progress over a specific duration, such as weeks, months, or even years. This type of evaluation provides an overview of

[43] ‘China Social Credit System Explained - How It Works [2023]’ (23 June 2022) <https://nhglobalpartners.com/china-social-credit-system-explained/> accessed 31 July 2023.

[44] Vera Lúcia Raposo, ‘Ex Machina: Preliminary Critical Assessment of the European Draft Act on Artificial Intelligence’ (2022) 30 International Journal of Law and Information Technology 88, 94.

how something has changed or developed over time. When evaluating something "episodically" however, one looks at the performance or progress in distinct episodes or events, such as during individual sessions or tasks. Episodic evaluation allows for a more detailed analysis of how something is performing in specific contexts or situations. Whether this kind of evaluation falls under the provision is unclear. It would be welcomed if further explanations are provided.

Finally, it is interesting that the original AIA texts (Art. 5 (1) lit. c) ii.) COM-AIA) imposes a conditionality: Social scoring systems are only prohibited if the data used for scoring is unrelated to the circumstances in which the data was originally generated or collected, or if the worse position is "unjustified or disproportionate." Consequently, the use of data that is derived from the same circumstances (better: the same social sphere) - e.g. an algorithm that assesses whether people are likely to commit crimes again based on their past criminal record - would not be prohibited.[45] The question of how compatible this is with human dignity and the presumption of innocence is obvious. The issue of predictive policing will be discussed below.

d) Real time remote biometric identification systems

Finally, "the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement" is also prohibited. This is because they would pose significant threats to fundamental rights, in particular for Articles 1, 7, 8 and 21 European Charter of Fundamental Rights (ECFR).[46] Nevertheless, in the Commissions and Council versions of the AIA exceptions in areas such as terrorism prevention, targeted search for specific persons like children exist, whereas Parliament wants to prohibit the practice altogether. Besides the question of whether to have exceptions at all or not, issues remain concerning the proposed wording (aa), unclear definitions (bb) and the question of "retroactive identification" (cc).

aa) Lower threshold for judicial or administrative authorization?, Art. 5 (3) COM-AIA

[45] Przemyslaw Palka (n 31) 5.

[46] European Commission, 'New Rules for Artificial Intelligence – Q&As' (*European Commission - European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683> accessed 13 April 2023.

The proposed exceptions to the prohibition apply "in so far as such use is strictly necessary" (Art. 5 lit d.) and appear to be exhaustive. *E contrario,* exceptions other than those mentioned cannot justify the use of real-time biometric remote identification systems in publicly accessible premises.[47] In any case, strict criteria are set out in Art. 5(2). The principle of proportionality and a fundamental reservation of the right of judges are explicitly mentioned and (Art. 5 (3)), Exceptions are permitted for a 'justified situation of urgency' whereby authorisation may then be requested during or after use, which in principle is in line with EU fundamental rights law, judgments of the CJEU, and ECHR case law[48] on the right to private life and secret surveillance under Article 8 of the European Convention on Human Rights.[49] However, as *Ni Loideain* rightly points out[50], the wording concerning prior judicial authorization in Art. 5 (3) subpara. (2) is confusing. It states that authorization shall be granted based on "objective evidence or clear indications" […] that the use is "necessary" […]. This points towards a lower threshold than the one established right above in Art. 5 (1) lit. (d) ("strictly necessary"). As such this is incoherent wording which however leads to major legal differences. It remains to be seen if this is simply a glitch in wording or an intentional political decision.

bb)Some unclear definitions and the question of "virtual spaces"

Besides some questions surrounding unclear definitions of biometric identification, the initially proposed wording in the COM-AIA arguably does not apply to the "virtual area", e.g. Youtube live streams. Unless courts teleologically expand the meaning of "publically accessible spaces" to encompass also the "virtual spaces", real-time remote identification seems possible there. This could lead to a situation where a YouTube live stream, which is publicly accessible over the internet, would be used for real time remote biometric identification of either the persons willingly appearing on that Youtube Stream or simply the randomly passing pedestrians or others. It is questionable whether the legislator

[47] Thomas Burri and Fredrik von Bothmer, 'The New EU Legislation on Artificial Intelligence: A Primer' [2021] SSRN Electronic Journal 2 <https://www.ssrn.com/abstract=3831424> accessed 11 April 2023.
[48] Nora Ni Loideain, 'The Approach of the European Court of Human Rights to the Interception of Communications' (25 September 2020) <https://papers.ssrn.com/abstract=3699386> accessed 13 April 2023; Nóra Ni Loideain, 'A Trustworthy Framework That Respects Fundamental Rights? The Draft EU AI Act and Police Use of Biometrics' (*Information Law & Policy Centre*, 4 August 2021) <https://infolawcentre.blogs.sas.ac.uk/2021/08/04/a-trustworthy-framework-that-respects-fundamental-rights-the-draft-eu-ai-act-and-police-use-of-biometrics/> accessed 13 April 2023.
[49] Ni Loideain (n 47).
[50] ibid.

wishes to open such a loophole. The only reference to a "virtual space" can be found in the EP-AIA , in the definition of AI itself: "artificial intelligence system' (AI system) means a machine-based system that […] generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments." This, however, does not resolve the question whether live streams in virtual spaces fall under the prohibition of remote biometric identification. A clarification during trilogues seems necessary.

cc) The issue of retractive identification, so called "post-systems" of identification

A major, long unaddressed issue is the question of retroactive biometric identification and predictive policing. Art. 5 COM-AIA only refers to "real-time remote identification systems". This means, as *Veale and Borgesius*[51] point out, that "post-systems" are not covered by the prohibition. In other words, it would be conceivable to subsequently and retroactively identify biometrically participants (in demonstrations for example) using AI systems. Yet, both real-time and ex-post identification system can violate citizens fundamental rights in equally substantive ways. As concisely reminded by the "European Digital Rights society" (EDRi) : "Over 200 civil society groups across Europe and globally, the EDPS and EDPB, the European Parliament and the UN High Commissioner for Human Rights have all highlighted the […] threat that the use of RBI in publicly accessible spaces, including online, poses to fundamental rights to privacy, data protection, equality, non-discrimination, freedom of expression and information, peaceful assembly and association, liberty, dignity, and the presumption of innocence, as well as to basic principles of democracy, media freedom and the rule of law."[52] Whether live or retroactively, both biometric identification systems can have a so called "chilling effect". This refers to a situation where individuals or groups are deterred or discouraged from exercising their rights or freedoms due to fear of negative consequences, such as retaliation or punishment. Such an effect could potentially lead to a culture of fear and self-censorship, where

[51] Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act — Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach' (2021) 22 Computer Law Review International 97, 101.

[52] EDRi et. al., 'The EU's Artificial Intelligence Act: Civil Society Amendments' (*European Digital Rights (EDRi)*) 2 <https://edri.org/our-work/the-eus-artificial-intelligence-act-civil-society-amendments/> accessed 13 April 2023.

people do not feel free to express themselves fully or engage in open debate and discussion. Whether you get to know during the demonstration that you are being biometrically identified or afterwards might not matter to the person concerned. In both situations it could discourage citizens to participate in a future demonstration. The differentiation between "real-time" and "post" identification becomes even more questionable when considering how "real time" is defined by the AIA itself: " 'real-time' remote biometric identification system' means a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention (Art. 3 (37))". Now, not only is not clear what "significant delay" or "limited short delays" mean, that is, when "real-time" identification becomes "post" identification. More importantly, where qualitative difference in terms of intrusiveness between identification with "significant delay" (= "real time" according to Art. 3 (37)) and "post" biometric identifications?

Although the European Parliament had adopted a firm position on biometric identification systems[53] and even explicitly mentions "post" systems as being prohibited (Art. 5 d (d) EP-AIA), some influential Member States in the Council are not so clear. The German government for example, although the governments coalition agreement[54] states differently, is reportedly against a ban on post identification systems.[55] This issue thus remains unresolved and controversial. Negotiations promise to be intense on this point.

e) Predictive policing – the problem of feedback loops

Civil society organisations[56] rightly remind us that, "Artificial intelligence (AI) systems are increasingly used by European law enforcement and criminal justice authorities to profile people and areas, predict supposed future criminal behaviour or occurrence of crime, and assess the alleged 'risk' of offending or criminality in the future. These predictions, profiles, and risk assessments, conducted against individuals, groups and areas

[53] 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.

[54] 'Ampel Koalitionsvertrag 2021' (*Die Bundesregierung informiert | Startseite*) <https://www.bundesregierung.de/breg-de/aktuelles/koalitionsvertrag-2021-1990800> accessed 13 April 2023., page ??

[55] Luca Bertuzzi, 'Germany Could Become MEPs' Ally in AI Act Negotiations' (*www.euractiv.com*, 9 January 2023) <https://www.euractiv.com/section/artificial-intelligence/news/germany-could-become-meps-ally-in-ai-act-negotiations/> accessed 13 April 2023.

[56] EDRi et. al. (n 51).

or locations, can influence, inform, or result in policing and criminal justice outcomes, including surveillance, stop and search, fines, questioning, and other forms of police control. They can lead to arrest, detention, prosecution, and are used in sentencing, and probation. They can also lead to other, civil punishments, such as the denial of welfare or other essential services, and increased surveillance from state agencies." In this respect, the EU's Agency for Fundamental Rights also released a report on bias in algorithms[57] warning about the very real threats that predictive policing can have to fundamental rights due to bias data and so called "feedback loops".

A feedback loop occurs when predictions made by a system influence the data that are used to update the same system.[58] Let's say, for example, there is an AI-powered music streaming service that recommends songs based on the user's listening history. The more the user listens to songs recommended by the service, the more data the service receives about the user's preferences, and the more accurate its recommendations become. This continuous cycle of receiving feedback from the user and adjusting its algorithms accordingly is a feedback loop in AI. To a certain extent the output of the AI thus becomes its future input.[59] This is extremely problematic in the context of predictive policing, especially if the initial data quality is already bias or if there is not enough reported datasets. Unfortunately, as another FRA reports shows, the report rate of crimes is influenced by victims' personal characteristics such as gender, ethnicity, age, religion and their socioeconomic background. For example, if predictions of crime rates are based on low reporting rates that fail to reflect the reality of crime occurrence, or the 'true crime rate', this can lead to false predictions and wrong policy decisions. In addition, the type of crime also influences the data. The FRA gives a good illustrative example: "Certain population groups may be more often associated with crimes that are easier to detect. This may lead to biased predictions over time, as predictions are overly focused on types of crime that are more readily recorded by the police. In addition, the police may behave differently in neighbourhoods that are assumed to have higher crime rates. An increased sense of vigilance among the police in such neighbourhoods may lead to an increase in observed crimes, which can also lead to biased crime records."[60] Against this background and since

[57] EFRA., *Bias in Algorithms: Artificial Intelligence and Discrimination.* (Publications Office 2022) <https://data.europa.eu/doi/10.2811/25847> accessed 13 April 2023.
[58] ibid 8.
[59] ibid.
[60] ibid 11.

predictive policy could be considered a high-risk AI system (see below), the Agency suggests clarifying Art. 10 (5) dealing with Data and Data governance of High Risk systems. Yet, even if measures concerning Data governance were to be clarified, the area of predictive policing remains highly sensitive and intrusive to fundamental rights. Not only is there little public information on how the algorithms have been trained, but even law enforcement officers might lack the skills to detect errors. Besides, just recently the German Federal Constitutional Court ruled[61] that predictive policing systems are unconstitutional as they violate the right to informational self-determination (Art. 2 (1) in conjunction with Art. 1 (1) *Grundgesetz*). Against this background and the high risk that wrong predictive policing could pose to fundamental rights, fair trial principles and the presumption of innocence, it seems desirable to add predictive policing to the enumeration of prohibited AI practices under Title II AIA. That is also what Parliament will defend in the coming trilogue (see Art. 5 d EP-AIA).[62] It can be expected that Council will clash with the Parliament's inclination in this respect.

2. High risk – High risk systems (Title III)

Title III of the AIA is dedicated to so-called high-risk systems. There are two ways an AI system is considered high risk. First, if it is a safety component of a product, itself the product or required to undergo third party conformity assessment pursuant to union harmonization legislation enumerated in Annex II. For example, if an AI system is incorporated into a toy, a lift, a watercraft, forestry vehicles or personal protective equipment (all of those and many more falling under harmonising secondary union legislation), then the product would be considered a High-risk AI system. Secondly, if an AI system falls under one of the systems enumerated in Annex III it is considered a high-risk system. Pursuant to Article 7 in conjunction with Article 73 COM-AIA, the Commission is authorised to amend Annex III. However, some classification criteria are legally anchored, which the Commission must follow (Art. 7 (2)). Chapter 2 of Title III sets out the legal requirements of high-risk AI systems with regard to a so-called "risk management system" (Art. 9),

[61] 'Bundesverfassungsgericht - Presse - Regelungen in Hessen Und Hamburg Zur Automatisierten Datenanalyse Für Die Vorbeugende Bekämpfung von Straftaten Sind Verfassungswidrig' <https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2023/bvg23-018.html;jsessionid=939761EDCFE19D29600C1DE4560C744B.internet952> accessed 13 April 2023.

[62] Access Now, 'EU Parliament's Draft of AI Act: Predictive Policing Is Banned, but Work Remains to Protect People's Rights' (*Access Now*) <https://www.accessnow.org/press-release/ai-act-predictive-policing/> accessed 13 April 2023.

data and data governance (Art. 10), technical documentation (Art. 11), record-keeping obligations (Art. 12), transparency and provision of information to users (Art. 13), human supervision (Art. 14) as well as requirements for the accuracy, robustness and cybersecurity of high-risk AI systems (Art. 15). The Commission emphasises[63] that these criteria come from the "tried and tested ethical guidelines" of the High-Level Expert Group on Artificial Intelligence. However, the AIA does not prescribe any fixed technical solutions but leaves the providers free to decide how the legal and technical requirements are achieved. There is a legal openness to technology not to hinder scientific and technological progress through unilateral regulation. Chapter 3 sets out horizontally applicable obligations for providers and partly for users of high-risk AI systems. Chapter 4 outlines the requirements for the bodies to be notified. Chapter 5 details the legal framework for the conformity assessment procedure. *Prima facie*, the proposal seems well thought out.
Yet, there remain some central elements that will be subject to further negotiation. In particular classification rules, data governance and human oversight.

a) Classification rules for high-risk AI systems

aa) Limited possibilities to amend the areas 1-8 of Annex III, Art. 7 AIA

AI systems used in the areas 1-8 of Annex III are considered high-risk. As mentioned above, the Commission is empowered to adopt delegated acts to amend the list of AI systems falling under the categories/areas 1-8 of Annex III (Art. 7). *E contrario*, novel AI systems that fall precisely outside the areas listed in Annex III cannot be classified by the Commission as high-risk applications. Similarly, to the reasoning given above in favour of a possibility to expand the list of prohibited applications (Art. 5), a rigid approach for high-risk AI systems is also questionable. Therefore, it seems desirable to empower the Commission to add new or to delete some areas of Annex III. Parliament has recognised this problem and filed amendments accordingly (see Art 7 (1) EP-AIA). It would only be sensible if the Council adopted a similar position during trilogue negotiations.

bb) Critical risk management by AI providers – the issue with self-assessment, Art.

[63] 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 2021 13.

9, 16 AIA

The risk management system prescribed in Art. 9 AIA is to assess known and foreseeable risks and take "appropriate" risk management measures to counteract possible hazards and risks (Art. 9 para. 2). According to Art. 9(4), these risk management measures should be designed in such a way "that any residual risk associated with a particular hazard as well as the overall residual risk of the high-risk AI systems can be assessed as acceptable". With regard to testing, Art. 9(6) also stipulates that testing procedures must be "appropriate". The problem here is, however, that the COM-AIA seemingly leaves it up to the providers to decide what is considered "reasonable" or "suitable". In other words, the decision on what risks is considered "reasonable" is delegated to the AI provider who is simultaneously trying to bring the AI system onto the market.[64] It's a self-assessment mechanism. This approach is different to the one's used in other tech legislation such as the Cyber Security Act (CSA).[65] In the CSA, unless we look at a low risk ICT product, the certification authorities are in charge of verifying compliance with the requirements set in the certification scheme.[66]

Sure, the benefit of a self-assessment is that the AI provider best knows the product and, consequently, can best certify its conformity.[67] But the arising risk of having an incomplete or incorrect self-assessment is obvious.

An alternative to a self-assessment system could be a third-party assessment. This, however, seems very burdensome. It would presumably create a huge backlog of conformity applications which would – especially in the beginning of AI development –inhibit innovation. This would in return undermine Europe's ambition to become the "global leader in developing cutting-edge, trustworthy AI"[68] it wants to be. Hence, this does not seem to be a viable option.

As an alternative, one could think of requesting AI providers to include a fundamental

[64] Smuha and others (n 33) 32.
[65] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance).
[66] Federica Casarosa, 'Cybersecurity Certification of Artificial Intelligence: A Missed Opportunity to Coordinate between the Artificial Intelligence Act and the Cybersecurity Act' (2022) 3 International Cybersecurity Law Review 115, 128.
[67] Raposo (n 43) 98.
[68] European Commission, 'A European Approach to Artificial Intelligence | Shaping Europe's Digital Future' (24 March 2023) <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence> accessed 14 April 2023.

rights impact assessment into their self-assessment. This would make sure that developers would deal *ex ante* with possible impacts of their system on fundamental rights. Such a fundamental rights assessment is now included in the Parliaments AIA version (Art. 9 (2) lit.a) and will certainly be pushed by the institution in the coming trilogues.[69] In case market behaviour in the coming years proves the stepped-up self-assessment to be insufficient, one could start thinking of a third-party assessment.

cc) The problem of value chains and allocation of responsibilities

Another fundamental problem concerns the value chain of an AI system. As the Centre of European Policy Studies (CEPS) outlines[70], the development of an AI system will generally, but not necessarily always, follow certain steps: first comes the problem definition, then data collection and pre-processing, model training, model retraining, model testing and evaluation, integration into software and finally the model deployment.

For the Commission's AI-Act version, the value chain is simple: the two main players are the provider and the user. Other mentioned parties in the AIA like the importers and distributors do not play a significant role.

A provider is defined as *"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" (Art. 3 (2) COM-AIA).*

For its part, *"'user' means any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity" (Art. 3 (4) COM-AIA).*

As CEPS illustratively explains[71], under these definitions, a provider is essentially the last entity to develop or integrate an AI system into a product or software before it is either sold or used. If the provider is selling the AI system, a user is any purchasing entity that then uses the software or product for any non-personal use. The differentiation between

[69] Luca Bertuzzi, 'AI Act: MEPs Want Fundamental Rights Assessments, Obligations for High-Risk Users' (*www.euractiv.com*, 10 January 2023) <https://www.euractiv.com/section/artificial-intelligence/news/ai-act-meps-want-fundamental-rights-assessments-obligations-for-high-risk-users/> accessed 14 April 2023.
[70] Alex Engler and Andrea Renda, 'Reconciling the AI Value Chain with the EU's Artificial Intelligence Act' (*CEPS*, 30 September 2022) 2 <https://www.ceps.eu/ceps-publications/reconciling-the-ai-value-chain-with-the-eus-artificial-intelligence-act/> accessed 15 April 2023.
[71] ibid 4.

providers and users is fundamental and of extreme importance as different legal responsibilities are placed on the provider and the user. This is especially true, when a provider becomes a high-risk AI systems provider (CEPS pointedly calls them PHRAIS). Providers of high-risk AI-systems have significantly more requirements to abide (risk management, data governance, transparency, documentation etc...). On the other hand, following the initial AI-Act proposal (Art. 28), a user can also become a provider when they use or place on the market the system under their trademark or name, modify the intended purpose or make a substantial modification to the AI-system. Consequently, they would be required to comply with the more complex provider requirements.

What first looks simple and clear however, is challenged by reality. Different business models exist on the AI market that do not neatly fit under this clear cut differentiation. Three examples[72] illustrate this very well: First, one can imagine a contractor developing an AI system for a company but without using it itself or placing it on the market. Since they didn't place the system on the market, the contractor is not a provider under the AIA. Instead, the buying company who puts the AI model to use or onto the market becomes the provider. In such a situation though, the buying company assumes potentially the highly technical PHRAIS responsibilities without having developed the AI system itself nor maybe understanding it even. How can they comply with the AIA if they did not develop the system and lack the technical understanding? Cooperation between the two entities and contractual terms will be key. A second example refers to a vendor writing code for an AI system but not pre-training it. The buyer is the one adding (it's) data to finish the AI system. Prima facie one could think that the vendor selling the software is the provider. However, since the vendor does not have the data (nor wants it) , one could argue that he has not even created an AI system as his software does not "generate output" (criterium needed for the existence of an AI system under the given definition in Art. 3 AIA) and hence he cannot be a provider of an AI system.[73] But even if the initial vendor is a provider, we would find ourself in a situation where the vendor has access and control over code, but not the data (again, because they might not want it even). Vice versa the buyer would have control over the data but no control over the code.[74] How this situation can comply with the AIA requirements is difficult to say. Close cooperation between the

[72] Alex Engler and Andrea Renda (n 69).
[73] ~~ibid 10.~~
[74] ~~ibid.~~

parties would have to take place. Third and last example illustrating business practices that challenge the AIA would be a situation where an initially developed AI system is fine-tuned by another entity without modifying the purpose or making substantial modification under Art. 28. If the initial AI system is high risk, then the initial developer would be considered a PHRAIS. If the fine tuning entity now places the fine tunes (but not substantial modified) model on the market the compliance responsibilities would still apply to the initial (broader model) developer. One could argue[75] that since the fine-tuning entity has access has full access to the AI system and is able to feed in new data and change the model need be, the responsibilities should at least be shared. *

Against this background of complex allocation questions, the Parliament calls on ~~for~~ the Commission "*develop and recommend non-binding model contractual terms between providers of high-risk AI systems and third parties […] in order to assist both parties in drafting and negotiating contracts with balanced contractual rights and obligations, consistent with each party's level of control"* (Art. 28 (2) lit. a EP-AIA).

In any case, ~~the above examples point out that~~ there are multiple types of value chains with two or more entities where neither entity has both control of all code and all data and compliance becomes difficult. The regulator should keep in mind that in reality the original AI developers are essentially big tech companies with lots of financial and technical resources and that they will have it easier with compliance than SME's and start-ups.

dd) Unfair contractual terms unilaterally imposed on an SME or startup, Art. 28a EP-AIA

Interestingly, the Parliament also proposes a whole new Article dealing with unfair contractual terms between an enterprise and a SME or startup, in other words B2B. Unlike in a business to consumer (B2C) relation where the European legislator presupposes the consumer to be the weaker party (and therefore has put in place numerous consumer protection law such as the Unfair Commercial Practices Directive (2005/29/EC), the Unfair Contract Terms Directive (93/13/EEC), the Consumer Rights Directive (2011/83/EU) and the Enforcement and Modernization Directive 2019/2161 also known as the Omnibus Directive) , in B2B relations the legislator has so far been mindful to respect the contractual freedom of the parties. Introducing a passage dealing with the B2B relationship is

[75] ~~ibid.~~

therefore unusual but shows that Parliament considers the future of AI to bring systematic imbalances between big enterprises and SME's and startups.

ee) The question of substantial modification, Art. 28 AIA

The initial Commission proposal foresees that any user (and others) will be considered a provider (and hence would have to abide with the high requirements of a high risk application) if they "modify the intended purpose" or "make a substantial modification to the high risk AI system" (Art. 28 (1) lit. c) . Likewise, "high-risk AI systems shall undergo a new conformity assessment procedure whenever they are substantially modified" (Art. 43 (4) (1)). The problematic term here is "substantially modified". Although Recital 23, 66 and Art. 43 (4) (2) try to further explain what this means, it still is not clear. It seems that the this would depend on the predetermined criteria the initial provider had given. In turn this might give him some margin to reduce his legal compliance duties.[76] As a matter of coherence though, the legislator is called upon to clarify these concepts. It is desirable to align the EU product liability regimes which undergoes a review with the AIA or vice versa. Same applies for the recently proposed AI liability directive.[77]

ff) Overall uncertainty related to AI classification

As a general remark, classification of AI systems is a difficult task. Recent research has shown that out of a sample of more than 100 AI applications 18% of the AI systems were found to fall into the high-risk class, 42% are low-risk, and for 40% it is unclear whether they fall into the high-risk class or not. Thus, the percentage of high-risk systems in this sample ranges from 18% to 58%.[78] This example clearly illustrates that there is still significant uncertainty as to how to classify the AI systems. The study suggests providing further guidance, clear instructions, more examples of classifications as well as binding and fast responses to questions regarding unclear classification via a central European portal.[79] This could be done by the AI board the regulation wants to establish (Art. 56).

---

[76] Alex Engler and Andrea Renda (n 69) 11.

[77] 'Proposal for a Directive on Liability for Defective Products | Internal Market, Industry, Entrepreneurship and SMEs' <https://single-market-economy.ec.europa.eu/document/3193da9a-cecb-44ad-9a9c-7b6b23220bcd_en> accessed 15 April 2023.

[78] Andreas Liebl and Till Klein, 'AI Act: Risk Classification of AI Systems from a Practical Perspective' (*appliedAI*) <https://www.appliedai.de/hub/ai-act-risk-classification-of-ai-systems-from-a-practical-perspective> accessed 14 April 2023.

[79] ibid 50.

Meanwhile it has been reported[80] that the European Parliament plans to introduce a new "lawyer" when classifying potentially high risk-AI applications. Instead of having an automatic high-risk classification, an AI system would only be considered as such if they pose a significant risk of harm to health, safety, or fundamental rights. If AI providers consider that their system does not pose a significant risk, thy would have to inform the competent national or European authority and provide reasoning. The authority would then have three months to object to the self-classification of provider. During this period the provider would still be able to launch their AI system on the European market though. On the one hand this would mitigate the concerns raised around the risk of abuse through the ex-ante self-assessment of AI providers (see above). On the other side it remains unclear if the authority must reply to each notification or not. An obligation of notification would inevitably lead to a huge backlog which would in turn impede on the authority's ability to identify the real problematic AI systems.

b) Data governance, Art. 10 AIA

Art. 10 (3) AIA provides that "training, validation and testing records must be relevant, representative, error-free and complete". This wording is problematic for two reasons. On the one hand, it is difficult to imagine ever finding "error-free and complete" datasets. In this respect, such legal requirements seem almost impossible to be complied with.[81] On the other hand, data integrity (in the sense of data origin) is not mentioned. The question therefore arises as to the status of data collected in violation of the rights of individuals outside the EU - e.g. data of the Chinese population with less extensive data protection rights - and whether their use would still be considered appropriate in the proposed regulation.[82] Besides, what about liability: who would be liable if incomplete or wrong data is used? The data provider? The AI system provider? The user?

c) Human oversight – who supervises the supervisor? Art. 14 AIA

The AI Act places a lot of responsibility onto human oversight to effectively prevent or

[80] Luca Bertuzzi, 'AI Act: EU Parliament Walking Fine Line on Banned Practices' (*www.euractiv.com*, 14 April 2023) <https://www.euractiv.com/section/artificial-intelligence/news/ai-act-eu-parliament-walking-fine-line-on-banned-practices/> accessed 16 April 2023.
[81] The Council seems to have detected the same problem and has added "to the best extent possible" in his general approach to the AIA.
[82] Smuha and others (n 33) 34.

minimalise the risks emerging from high-risk AI tools. While *prima facie* human oversight of risky AI systems is a good thing one can ask further: Who supervises the supervisor? This question becomes ever more relevant if one acknowledges with *Johannes Walter et alia.*[83]*,* that humans are actually not so good at overseeing and critically assessing what an algorithm tells them. Arguably this lack of critical assessment can be attributed to a feeling that AI recommendations seem objective and thus makes it more difficult to go against them. This could lead to what is referred to as "algorithmic appreciation" , whereby humans rely too much on algorithms. At the same time the opposite can also occur: "algorithmic aversion" whereby humans "erroneously do not follow superior algorithmic advice".[84] The researchers propose introducing different kinds of tests to assess the efficacy of human oversight. Indeed, this seems sensible, especially in the area of high-risk applications. It remains to be seen if the EU institutions follow this sensitive proposal.

3. General Purpose AI, Foundational models, Generative AI and the Chat GPT Effect

The elephant in the room these last months has been what to do with General-Purpose AI, foundational models and generative AI.

Unlike Artificial narrow intelligence (ANI) which is pretty good at performing a given task in a predefines environment and trained on task-specific datasets, Artificial general Intelligence (AGI) can adapt to new situations, new information, reason and solve problems, communicate, and interact with human in a natural way and create new knowledge. Chat GPT and similar Large Language Models have increased awareness of the regulatory difficulties and risks of AIA. In addition to copyright violations, hate speech, and biases in training data, potential risks include an avalanche of well-written and plausible-sounding disinformation designed to manipulate public opinion. Leading AI and ethics experts have therefore signed articles and manifests calling for a halt to AI development and a more circumspect approach in general. (Future of Life Institute, AI Safety Centre,

[83] Jan Biermann, John J Horton and Johannes Walter, 'Algorithmic Advice as a Credence Good' [2023] SSRN Electronic Journal <https://www.ssrn.com/abstract=4326911> accessed 14 April 2023; Johannes Walter, 'The AI Act Should Use Humans to Monitor AI Only When Effective' (*www.euractiv.com*, 15 February 2023) <https://www.euractiv.com/section/digital/opinion/the-ai-act-should-use-humans-to-monitor-ai-only-when-effective/> accessed 14 April 2023.

[84] Walter (n 88).

State of AI, Harrari, etc.) In AI, it is becoming increasingly apparent that foundational models, generative AI, and AGI play an indispensable role.

a) The initial Commissions proposal did not address foundational models, generative AI or AGI

The initial Commission proposal did not explicitly mention general AI or general-purpose AI. Especially in the category of high-risk AI, into which one might assume such AI would fall, no mention can be found. This does not necessarily mean that general purpose AI is not covered by the AIA. Yet, it has rightly been demonstrated[85] that as things stand under the initial Commission proposal, General-Purpose AI will not have to abide by high-risk AI requirements. First and foremost, it is highly doubtful that a General-Purpose AI provider will have an intended purpose that qualifies as a high-risk application pursuant Annex III. As shown above, without intended purpose in one of the stated areas of Annex III, the AI system will not be regarded as high-risk. In addition, if a General Purpose AI is put on the market it will most probably be adapted, fine-tuned and changed. This potentially leads to a substantial modification under Art. 28 COM-AIA which in turn would pose the obligations of high risk systems onto the secondary developer. The initial GPAI will be left blank. This seems counterintuitive as it is the initial GPAI that provides an essential foundation for the secondary, fine-tuned model. Hence, it may be sensible to require the initial GPAI also respect the high-risk AI systems requirements that intend to safeguard amongst others the quality of data and fundamental rights. Indeed, the initial COM-AIA is conceptually deficient when it comes to foundational models.

b) The Council's wants a new Title Ia

Presumably against this background, the Council proposes a new Title Ia (Art. 4a, b and c) specifically aimed at regulating "General purpose AI".[86] Three major aspects of the Councils proposal are worth discussing. First, the text reads that "General purpose AI systems which may be used as high-risk AI systems or as components of high-risk AI systems in the meaning of Article 6, shall comply with the requirements established in Title III, Chapter 2". This is a substantial difference to Art. 6 and 7 AIA where an intended purpose is required. The Council text thus is much wider as it also incorporates models

[85] Alex Engler and Andrea Renda (n 69) 18.
[86] Council General approach - 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 (n 29).

that could potentially be used as high-risk systems. A clear intention is not required. The initial GPAI from the above given example would thus be covered. At the same time, however, the Council also unequivocally incorporates (see recital 1a) Open Source GPAI models. These are models mostly created by research institutions and uploaded online as open-source systems. Reasons of why an exemption for open-source AI models should be introduced are provided by *Engler and Renda*[87]. They mostly refer to possibilities of collective development, improvement, public evaluation, scrutiny and scientific research. But besides these valid reasons, it also seems incoherent from the Council to be excluding the from the application of the AIA "*AI systems, specifically developed, and put into service for the sole purpose of scientific research and development"*[88] (see above C. I. 2. b) and at the same time incorporating open source models that are for the vast majority research driven.

Secondly, instead of an "immediate" application of the requirements for high-risk systems, the Commission must specify in an implementing act how the requirements set out in Title III chapter 2 (High risk) should be applied to general purpose AI systems (Art. 4b (1)). In essence, GPAI providers - unlike other high-risk providers - are "given a hand" by the Commission. This will certainly be welcomed by GPAI providers who will not only (to a certain extent) get personalised guidance by the European executive but will also be blessed with quasi automatic legal certainty that their conformity assessments are compliant with EU law, since they are being instructed by the Commission herself on what to do. Thirdly, slightly contradictory with the aim of covering the initial GPAI developer, the Council wants to introduce an exception whereby "Article 4b shall not apply when the provider has explicitly excluded all high-risk uses in the instructions of use or information accompanying the general-purpose AI system." This exclusion is to be made in "good faith" and the provider shall still take necessary measures if he is informed about "market misuse". What market misuse means is not clear. Also surprises the fact that a mere contract disclaimer can unbind the initial GPAI provider from his legal obligations under the AIA. Maybe the Council and its Member States will clarify what reasoning can be found behind this.

[87] Alex Engler and Andrea Renda (n 69) 29.

[88] Council General approach - 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 (n 29) art 2 (6) and (7) respectively.

c) Parliament proposes a new Art. 28b

Finally, Parliament also found its own response on the matter. A new Art. 28b EP-AIA deals in depth with "foundational models". It sets nine obligations on development and design of the models and quality management systems. For instance, Article 28b (2a) would require the identification and reduction of foreseeable risks like inaccuracy and bias. This would need to be done with help from independent experts. Article 28b (2e) would also require substantial documentation like data sheets and model cards, as well as clear instructions for use. This documentation would help those who refine or fine-tune AI systems built on these foundation models to better understand what they are working with. Overall, these articles would mandate proper design, documentation, and risk mitigation for foundational AI models to enable safer downstream use.

A whole new paper would have to be dedicated to the question on how to regulate foundational models and General Purpose AI systems, which would go beyond the reasonable scope of this paper. One remark shall be allowed though: The institutions are advised to start settling on what they actually want to regulate and how they call it. While Council aims at regulating "general purpose AI", Parliament speaks of "foundational models". These are two distinct concepts with different implications. Also, the legislator should keep in mind that introducing a broad definition of "foundational model" as is now proposed by the Parliament would make compliance with Art. 28 b EP-AIA mandatory for every actor that works on foundation models. This in turn could further consolidate the market dominance of big companies such as OpenAI, Anthropic, Google DeepMind and alienate smaller actors working on foundational models.[89] These big companies already have a considerable lead in R&D and the financial means and support to become AI Act compliant rather quickly. Against this background and as *Zenner*[90] proposes, utilizing the Digital Services Act (DSA) approach also in the AIA framework sounds convincing. The Digital Services Act allows the European Commission to designate certain Very Large Online Platforms (VLOPs) and Search Engines (VLOSEs) based on specific criteria. These designated entities then have to follow additional compliance rules. A similar approach could be taken in the AI Act to define a category of Systemic Foundation Models that would fall under Article 28b. Using the term "systemic" would clarify that

[89] Kai Zenner, 'A Law for Foundation Models: The EU AI Act Can Improve Regulation for Fairer Competition - OECD.AI' <https://oecd.ai/en/wonk/foundation-models-eu-ai-act-fairer-competition> accessed 27 July 2023.
[90] ibid.

only a small number of highly capable and relevant foundation models would be subject to these extra requirements in Article 28b. This would target regulation at the most powerful and systemically important foundation models, just as the VLOP/VLOSE designations do for online platforms and search engines under the Digital Services Act (Art. 33 (4) DSA)

4. "Low or minimal risk" - certain (other) AI systems (Title IV)

Title IV establishes transparency obligations for "certain AI systems". In particular, systems that either interact with humans, recognise emotions, generate or manipulate content are taken into consideration. The latter explicitly refers to so-called deepfakes (Art. 52 (3) COM-AIA). The transparency obligations imposed include above all the duty to disclose that the AI application is one that manipulates image, audio or video files and thus distorts perception. Again, exceptions apply to "AI systems authorised by law for the detection, prevention, investigation and prosecution of criminal offences".

A closer look at the risk-based regulatory system of the draft regulation and the accompanying documents reveals one thing: In its "New rules for Artificial Intelligence - Questions and Answers" press release[91] , the Commission still listed four risk spheres: in addition to the mentioned unacceptable applications (Title II) and the high-risk systems (Title III), the press release provided for two further spheres: low and minimal risk. Such a differentiation is not kept in the legislative proposal, which follows a three-tier model:Prohibited applications (Title II), high-risk applications (Title III) and "certain AI applications" (Title IV). Nevertheless, by "low risk" the Commission probably means Title IV, which prescribes transparency obligations for "certain AI applications". With "minimal risk", a kind of catch-all is created for all AI systems not covered by the other risk spheres - i.e. those that ultimately lie outside the AIA framework. The latter are not subject to mandatory law. However, Art. 69 AIA encourages the establishment of voluntary codes of conduct. In this way, the AIA prevents national AI regulations and the fragmentation of the single market: a waiver of legally binding regulations also contains a decision not to regulate, which would be thwarted if the national legislator were to take action in this respect. In this respect, the AIA protects "minimal-risk applications" from other regulation. However, this does not change the need for clarification between the different risk spheres.

[91] Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682

Finally, it can be pointed out that there is a regulatory gap between "high-risk AI systems" (Title III) and "certain AI systems" (Title IV). While the requirements for high-risk systems are understandably correspondingly strict, the provisions of Title IV are modest. On the one hand, this may be justified as only only AI applications that really pose a threat to fundamental rights should be subject to strict requirements. On the other hand, there is also the danger that due to the lack of an intermediate level, many an AI system "slips" (too) quickly into the high-risk sphere. This in turn would run counter to the concern for legal certainty, would be anti-innovation and would place an above-average burden on small and medium-sized enterprises (SMEs). Whether such a risk will materialise remains to be seen. In any case, a discussion on a further differentiation between high-risk systems and "certain" systems would be appropriate.

5. Enforcement of legal requirements and legal protection

Finally, there is also the question of effective enforcement.

a) New European Artificial Intelligence Board, Art. 56 AIA

It seems particularly interesting that the regulation establishes a European Artificial Intelligence Board (or AI Office as Parliament wants to rename it) at Union level, similar to the to the European Data Protection Board created by the GDPR and the European Board for Digital Services under the DSA. Both the European Data Protection Supervisor and a representative of each of the national AI supervisory authorities are to be members of this committee. Whether the member states create a new national AI supervisory authority or rather restructure an existing department into their supervisory authority is up to them. In any case, this European Committee for Artificial Intelligence is to advise and support the Commission. In particular, it should work towards a uniform administrative practice and ensure the exchange of "best practices". Such a governance structure at the Union level seems only logical with the adoption of a uniform legal framework. However, special care will have to be taken to make the communication channels as effective as possible in order to avoid bulky duplicate structures as far as possible. This is why the central question of how far-reaching the competencies of this newly created board will be is interesting.

One can expect a (classical) power struggle between those in favour of a decentralized

enforcement mechanisms (mostly the Council) and proponents of a more centralized approach. In order to avoid divergences in the enforcement practice and not end up with GDPR-style enforcement solutions that have significant room for improvement, one might consider that a centralized approach is better. This however comes with significant financial burdens for the EU budget. While the Council seems naturally more inclined to limit powers of yet another supranational body, Parliament has been pushing for a strong AI "Office". Let's see how that one plays out.

b) Lack of complaints mechanism

Unlike the GDPR, the COM-AIA does not contain a complaint mechanism for individuals that would enable them to lodge a complaint with the competent authority. The GDPR, on the other hand, provides that each supervisory authority has the task to "deal with complaints lodged by a data subject or an institution, organisation or association pursuant to Article 80 and, where appropriate, investigate the subject matter of the complaint and inform the complainant of the progress and outcome of the investigation within a reasonable period of time, in particular where further investigation or coordination with another supervisory authority is necessary". While the AIA does not preclude national competent authorities from setting up a complaint mechanism on their own initiative, different national complaint mechanisms would potentially lead to different levels of protection between member states. Individuals would not be equally protected across the Union. The inclusion of a harmonised complaints mechanism, similar to the mechanism of the GDPR, would certainly strengthen individual rights protection. It would also contribute to the rule of law across the Union and help national authorities fight non-compliant AI applications. [92] The Council has also identified the lack of such a lack to take legal action and has added a new Article 63 (11) in its general approach. Parliament too added a new Article 68 (a) giving natural persons and groups the right to lodge a complaint with the national authority. Although the details are still to be agreed upon, this is a good step forward.

6. The AIA Innovation Brake - Measures to Promote Innovation

[92] Smuha et alia, how the eu can achieve legally trustworthy AI, p. 45,46

It is still questionable whether the planned regulation will not become a brake on innovation. After all, unnecessary regulation creates bureaucracy, additional costs for companies, which, when investing in research and development, affects innovation and the company's international competitiveness. Against this background, the Commission has sought to create "a regulatory framework that is innovation-friendly, future-proof and resilient." To this end, Title V contains measures to promote innovation. For example, "AI reallabs" also known as sandboxes are to be created. These "provide a controlled environment to facilitate the development, testing and validation of innovative AI systems for a limited period of time before they are placed on the market or put into service according to a specific plan" (Art. 53 (1) AIA). The aim is thus - as recital 72 makes clear - to promote innovation, ensure legal certainty and react quickly to new risks that arise. But the Commission also wants to relieve small providers and small users. Thus, with Art. 55 AIA, it is striving to ensure priority access for small providers and start-ups. Whether this will be enough to lead to more innovation rather than less remains to be seen. It is to be hoped that the transparency and documentation requirements (e.g. Art. 16, 18, 22 AIA) will not turn the AIA into a "bureaucratic monster" - in analogy to the frequently voiced criticism of the GDPR. In any case, the Commission is showing awareness of the problem and is signalling that it wants to counter the danger of a loss of innovation. From the Councils side new provisions have been added (Art. 54a and b) to clarify how rules are to interpreted. In addition, the Council proposes a cap on caps on the amount of administrative fines for SMEs and start-ups (Art. 71) certainly with the aim to easy the potential burdens on these players.

The European Commission and Council proposals for the AI Act allow EU member states the option to establish regulatory sandboxes for AI if they choose to. However, the European Parliament's version would require each member state to set up at least one national-level sandbox. The Parliament's text also clearly states that sandboxes could additionally be created at regional/local levels or jointly between multiple member states. This mandatory national sandbox, with the possibility of more at sub-national or multi-country levels, is seen as a positive push to foster AI innovation across the European Union more broadly.

D. Conclusion

The aim of this paper was to provide a holistic overview of some chosen prominent open questions the current AI text poses ahead of the upcoming trilogue negotiations. The main takeaway points are that while the co-legislators have already found common ground on some issues, they must still agree on the definition of AI, the list of prohibited AI systems and exceptions thereof, AI-value chains, classification and fundamental rights assessments, and foundational models. In any case the upcoming trilogue negotiations should be followed closely by all stakeholders . The AI-Act remains a fundamental future piece of European legislation arguably impacting the development of AI like no other legislation before. Only if done the right way can Europe carve out a global brand for trustworthy AI made in Europe and create another ”Brussels effect”, setting standards not only for Europe but de facto also for the world.

Bibliography

Access Now, 'EU Parliament's Draft of AI Act: Predictive Policing Is Banned, but Work Remains to Protect People's Rights' (*Access Now*) <https://www.accessnow.org/press-release/ai-act-predictive-policing/> accessed 13 April 2023

Alex Engler and Andrea Renda, 'Reconciling the AI Value Chain with the EU's Artificial Intelligence Act' (*CEPS*, 30 September 2022) <https://www.ceps.eu/ceps-publications/reconciling-the-ai-value-chain-with-the-eus-artificial-intelligence-act/> accessed 15 April 2023

'Ampel Koalitionsvertrag 2021' (*Die Bundesregierung informiert | Startseite*) <https://www.bundesregierung.de/breg-de/aktuelles/koalitionsvertrag-2021-1990800> accessed 13 April 2023

'Assessment List for Trustworthy Artificial Intelligence (ALTAI) for Self-Assessment | Shaping Europe's Digital Future' (17 July 2020) <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment> accessed 18 April 2023

Bertuzzi L, 'Germany Could Become MEPs' Ally in AI Act Negotiations' (*www.euractiv.com*, 9 January 2023) <https://www.euractiv.com/section/artificial-intelligence/news/germany-could-become-meps-ally-in-ai-act-negotiations/> accessed 13 April 2023

——, 'AI Act: MEPs Want Fundamental Rights Assessments, Obligations for High-Risk Users' (*www.euractiv.com*, 10 January 2023) <https://www.euractiv.com/section/artificial-intelligence/news/ai-act-meps-want-fundamental-rights-assessments-obligations-for-high-risk-users/> accessed 14 April 2023

——, 'EU Lawmakers Set to Settle on OECD Definition for Artificial Intelligence' (*www.euractiv.com*, 7 March 2023) <https://www.euractiv.com/section/artificial-intelligence/news/eu-lawmakers-set-to-settle-on-oecd-definition-for-artificial-intelligence/> accessed 12 April 2023

——, 'AI Act: EU Parliament Walking Fine Line on Banned Practices' (*www.euractiv.com*, 14 April 2023) <https://www.euractiv.com/section/artificial-intelligence/news/ai-act-eu-parliament-walking-fine-line-on-banned-practices/> accessed 16 April 2023

Biermann J, Horton JJ and Walter J, 'Algorithmic Advice as a Credence Good' [2023] SSRN Electronic Journal <https://www.ssrn.com/abstract=4326911> accessed 14 April 2023

Bradford A, *The Brussels Effect: How the European Union Rules the World* (1st edn, Oxford University Press 2020) <https://academic.oup.com/book/36491> accessed 12 April 2023

‘Bundesverfassungsgericht - Presse - Regelungen in Hessen Und Hamburg Zur Automatisierten Datenanalyse Für Die Vorbeugende Bekämpfung von Straftaten Sind Verfassungswidrig’ <https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2023/bvg23-018.html;jsessionid=939761EDCFE19D29600C1DE4560C744B.internet952> accessed 13 April 2023

Burri T and von Bothmer F, ‘The New EU Legislation on Artificial Intelligence: A Primer’ [2021] SSRN Electronic Journal <https://www.ssrn.com/abstract=3831424> accessed 11 April 2023

Casarosa F, ‘Cybersecurity Certification of Artificial Intelligence: A Missed Opportunity to Coordinate between the Artificial Intelligence Act and the Cybersecurity Act’ (2022) 3 International Cybersecurity Law Review 115

‘China Social Credit System Explained - How It Works [2023]’ (23 June 2022) <https://nhglobalpartners.com/china-social-credit-system-explained/> accessed 31 July 2023

‘Communication: Building Trust in Human Centric Artificial Intelligence | Shaping Europe’s Digital Future’ (8 April 2019) <https://digital-strategy.ec.europa.eu/en/library/communication-building-trust-human-centric-artificial-intelligence> accessed 18 April 2023

‘Coordinated Plan on Artificial Intelligence | Shaping Europe’s Digital Future’ (7 December 2018) <https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence> accessed 18 April 2023

‘EDPB-EDPS Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) | European Data Protection Board’ <https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en> accessed 16 April 2023

EDRi et. al., ‘The EU’s Artificial Intelligence Act: Civil Society Amendments’ (*European Digital Rights (EDRi)*) <https://edri.org/our-work/the-eus-artificial-intelligence-act-civil-society-amendments/> accessed 13 April 2023

‘EESC Opinion on the Artificial Intelligence Act’ (*European Economic and Social Committee*, 26 March 2021) <https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/regulation-artificial-intelligence> accessed 16 April 2023

EFRA., *Bias in Algorithms: Artificial Intelligence and Discrimination.* (Publications Office 2022) <https://data.europa.eu/doi/10.2811/25847> accessed 13 April 2023

‘Ethics Guidelines for Trustworthy AI | Shaping Europe’s Digital Future’ (8 April 2019) <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> accessed 18 April 2023

European Commission, ‘A European Approach to Artificial Intelligence | Shaping Eu-

rope's Digital Future' (24 March 2023) <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence> accessed 14 April 2023

——, 'New Rules for Artificial Intelligence – Q&As' (*European Commission - European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683> accessed 13 April 2023

'European Council Conclusions, 19/10/2017' <https://www.consilium.europa.eu/en/press/press-releases/2017/10/20/euco-conclusions-final/> accessed 18 April 2023

Grady P, 'The AI Act Should Be Technology-Neutral'

Hacker P, 'AI Regulation in Europe' [2020] SSRN Electronic Journal <https://www.ssrn.com/abstract=3556532> accessed 11 April 2023

——, 'Manipulation by Algorithms. Exploring the Triangle of Unfair Commercial Practice, Data Protection, and Privacy Law' [2021] European Law Journal eulj.12389

Kertysova K, 'Artificial Intelligence and Disinformation: How AI Changes the Way Disinformation Is Produced, Disseminated, and Can Be Countered' (2018) 29 Security and Human Rights 55

Liebl A and Klein T, 'AI Act: Risk Classification of AI Systems from a Practical Perspective' (*appliedAI*) <https://www.appliedai.de/hub/ai-act-risk-classification-of-ai-systems-from-a-practical-perspective> accessed 14 April 2023

Mitchell TM, *Machine Learning* (McGraw-Hill 1997)

Nemitz P, *Prinzip Mensch: Macht, Freiheit Und Demokratie Im Zeitalter Der Künstlichen Intelligenz* (Dietz 2020)

Ni Loideain N, 'The Approach of the European Court of Human Rights to the Interception of Communications' (25 September 2020) <https://papers.ssrn.com/abstract=3699386> accessed 13 April 2023

Ni Loideain N, 'A Trustworthy Framework That Respects Fundamental Rights? The Draft EU AI Act and Police Use of Biometrics' (*Information Law & Policy Centre*, 4 August 2021) <https://infolawcentre.blogs.sas.ac.uk/2021/08/04/a-trustworthy-framework-that-respects-fundamental-rights-the-draft-eu-ai-act-and-police-use-of-biometrics/> accessed 13 April 2023

'Opinion of the European Committee of the Regions — European Approach to Artificial Intelligence — Artificial Intelligence Act (Revised Opinion)' <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021AR2682#:~:text=High%2Drisk%20AI%20systems%20should,market%20or%20putting%20into%20service.>

'Policy and Investment Recommendations for Trustworthy Artificial Intelligence | Shap-

ing Europe's Digital Future' (26 June 2019) <https://digital-strategy.ec.europa.eu/en/library/policy-and-investment-recommendations-trustworthy-artificial-intelligence> accessed 18 April 2023

'Proposal for a Directive on Liability for Defective Products | Internal Market, Industry, Entrepreneurship and SMEs' <https://single-market-economy.ec.europa.eu/document/3193da9a-cecb-44ad-9a9c-7b6b23220bcd_en> accessed 15 April 2023

Przemyslaw Palka, 'The Phantom Menace: A Critique of the European Commission's Artificial Intelligence Act Proposal, Przemyslaw Palka' <https://law.yale.edu/yls-today/yale-law-school-events/phantom-menace-critique-european-commissions-artificial-intelligence-act-proposal-przemyslaw-palka> accessed 12 April 2023

Raposo VL, 'Ex Machina: Preliminary Critical Assessment of the European Draft Act on Artificial Intelligence' (2022) 30 International Journal of Law and Information Technology 88

Smuha NA and others, 'How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act' [2021] SSRN Electronic Journal <https://www.ssrn.com/abstract=3899991> accessed 12 April 2023

Veale M and Zuiderveen Borgesius F, 'Demystifying the Draft EU Artificial Intelligence Act — Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach' (2021) 22 Computer Law Review International 97

Walter J, 'The AI Act Should Use Humans to Monitor AI Only When Effective' (*www.euractiv.com*, 15 February 2023) <https://www.euractiv.com/section/digital/opinion/the-ai-act-should-use-humans-to-monitor-ai-only-when-effective/> accessed 14 April 2023

'White Paper on Artificial Intelligence: A European Approach to Excellence and Trust' <https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en> accessed 18 April 2023

Zenner K, 'A Law for Foundation Models: The EU AI Act Can Improve Regulation for Fairer Competition - OECD.AI' <https://oecd.ai/en/wonk/foundation-models-eu-ai-act-fairer-competition> accessed 27 July 2023

Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts [(COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))1]

Communication From The Commission To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions Artificial Intelligence for Europe 2018

Council General approach - 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 2022

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

Opinion of the European Central Bank of 29 December 2021 on a proposal for a regulation laying down harmonised rules on artificial intelligence (CON/2021/40) 2022/C 115/05 2021

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 2021

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 (General Data Protection Regulation

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)