

Deutscher Bundestag

Ausschuss für Digitales

Ausschussdrucksache

20(23)84

26.09.2022

AIA | Q&A (F&A)

**Hearing on the EU regulation on
artificial intelligence
German Bundestag**

***Anhörung zur EU-Verordnung zu
Künstlicher Intelligenz
Deutscher Bundestag***



Authors:

Catelijne Muller, LL.M

Noah Schöpl

INTRODUCTION

Thank you for the invitation to address the Ausschuss für Digitales of the Deutscher Bundestag during the hearing on the EU regulation on artificial intelligence on September 26, 2022 (*Anhörung zur EU-Verordnung zu Künstlicher Intelligenz*).

In preparation for the hearing, I received a *Fragencatalog* of 18 questions, which I will gladly answer in this paper.

For in-depth analyses of the proposal for the Artificial Intelligence Regulation ("AIA") I kindly refer to a [series of in-depth papers on the AIA](#) prepared together with my team at ALLAI:

- AIA in-depth #1 | Objective, Scope, Definition
- AIA in-depth #2 | Prohibited AI Practices
- AIA in-depth #3 | High Risk AI Classification
- AIA in-depth #4 | High Risk AI Requirements

While this paper will be in English, it will be translated into German upon request.

Catelijne Muller, September 25, 2022

About Catelijne Muller and ALLAI

Catelijne Muller has been involved in the AI policy processes at EU and international level since 2017. As AI-Rapporteur of the European Economic and Social Committee, she presented the [EESC opinion AI & Society](#) in 2017. This opinion is widely seen as the 'inflection point' at which Europe entered its path towards human-centric and trustworthy AI.

She was invited to sit on the EU High Level Expert Group on AI, and played an active role as co-rapporteur of the Policy and Investment Recommendations for AI and co-lead of the [Assessment List for Trustworthy AI](#), two of the three deliverables of the AI HLEG.

Catelijne Muller has a strong legal background and is considered an expert on the legal implications of AI, including human/fundamental rights and upcoming legislation such as the AI Act and the Data Governance Act, as well as anticipated proposals regarding AI liability, algorithmic management (Platform Workers) and the AI Convention of the Council of Europe. She has been advising the Council of Europe's CAHAI on the impact of AI on human rights, democracy and the rule of law. Her paper '[The Impact of AI on Human Rights Democracy and the Rule of Law](#)' now serves as a basis for the AI Convention. She continues as AI Rapporteur of the EESC and presented the opinions on the European Commission White paper on AI and the AI Act.

During the HLEG AI's mandate, she founded [ALLAI](#) together with two other members of the HLEG AI, Prof. Virginia Dignum and Prof. Aimee van Wynsberghe. Prof. Dignum and Prof. Van Wynsberghe were co-rapporteurs of the [Ethics Guidelines for Trustworthy AI](#), the third main deliverable of the HLEG AI.

ALLAI is an independent organisation dedicated to Responsible AI. ALLAI's mission is to take a holistic approach to AI, taking into account all impact domains such as economics, ethics, privacy, laws, safety, labour, education, etc. ALLAI aims to involve all stakeholders in its mission: policy-makers, industry, social partners, consumers, NGOs, educational and care institutions, academics from various disciplines.

ALLAI contributes to the policy process through direct advisory to EU and national policy makers, in-depth policy papers and the organisation of and participation in policy events, roundtables and panels.

AIA | Q&A (F&A)

Below please find the answers to the 18 questions of the *Fragencatalog*, sent in anticipation of the hearing.

- 1) In respect of case-by-case and sector-by-sector identification of risks and threats and the wish of, for example, business associations regarding sandboxes and a combination of *ex ante* self-assessment of risks and *ex post* enforcement for AI classed as high risk, the following questions arise, especially with regard to the Commission recommendation on the use of AI in public services as a “testing environment”: to what extent and by what means can it be assured that:
- no damage occurs in spite of the combination of two or more applications, particularly when used in critical infrastructure?
 - the severity of potential hazard situations can be ascertained, including consideration of cross-sectoral interfaces?
 - general questions of liability can be cleared up and possible gaps in security can be found, reported and swiftly remedied?

Ex ante, ex durante, ex post

The fact that the impact of AI on health, safety and/or fundamental rights is often 'hidden' or unknown and only discovered 'after the fact' means that the AIA should hold *ex ante*, but also an *ex durante* and *ex post* assessment and monitoring obligations.

Combinations of AI systems, critical infrastructure

The AIA currently does not contain any rules to assess and address the situation where combinations of AI systems that are in itself not prohibited or high risk, but in (cross-sectoral) combinations could pose unacceptable or high risks to health, safety or fundamental rights. Additional wording to that effect should be included, to ensure that the risk of harm/damage is avoided. AI used for the management and operation of critical infrastructure is considered high risk, but missing from this 'area' are AI systems used in the management and operation of the telecom, internet and financial infrastructure and the management, generation and supply of electricity and energy (including nuclear power).

Selective sectoral approach

Article 2 paragraph 2 AIA holds a noteworthy blanket exclusion of AI systems used in the aviation, vehicle, marine and railroad sectors. High risk AI systems in these domains are excluded from the scope of the AIA (with the exception of art. 84). The Commission wants to avoid interfering with existing governance, assessments and authorities already established in these sectors. The Commission deems it more appropriate to take into account the mandatory requirements for high risk AI systems laid down in the AIA, when adopting any relevant future delegated or implementing acts on the basis of the rules underpinning these domains.

This reasoning is confusing, because for other domains/sectors that also have strict requirements and procedures, (such as medical devices, lifts, toys etc.) this approach is not chosen. For these sectors, the AIA simply states that the requirements are to be included in existing procedures.

To understand the implications of this selective sectoral approach, it is good to consider what kind of AI systems would not directly be covered by the AIA, such as AI that is used to ensure the overall security of civil aviation, such as airport security and the selection of aviation staff. This means that AI-driven surveillance, profiling, crowd monitoring, behaviour assessment, hiring and firing in the aviation sector would not be covered by the AIA, until the sectoral rules are amended. The same goes for example for AI for driver behaviour monitoring in the automotive sector. For this reason, it becomes more difficult to clear up general questions of liability and find, report and remedy gaps in security effectively.

AI Liability Directive

This Wednesday, the European Commission will present a proposal for a Directive on Liability for AI. While the contents of this proposal are not yet known, legal scholars argue that non-compliance with the AIA would in fact cause liability under general (tort) liability rules. For this reason alone, in particular the selective sectoral approach could prove to be problematic.

- 2) In the area of blockchain technology, leading crypto experts have written a letter to the US Congress calling for regulation of crypto-assets and scrutiny of the added value engendered by using blockchain technologies. In the area of AI applications, the assumption is that there will be extensive challenges involved in regulating algorithms to shape socio-economic and environmental implications. Is it possible to ensure, in respect of both technologies, that they are applied in an appropriate manner in line with cost-benefit analysis, e.g. with regard to the environmentally sound consumption of resources or the generation of genuine added value in comparison to conventional IT applications, and, if yes, what measurable criteria are used for this and are the societal/social ramifications adequately taken into account?

The escalating 'risk pyramid' (from limited and medium-risk, to high risk, to unacceptable risk) used to categorise a number of AI practices as well as a number of domain/sector specific AI use cases, acknowledges that not all AI poses risks and not all risks are equal. The descriptions of the various prohibited AI practices and medium and high risk AI use cases, however, are at times unclear, multi-interpretable and could lead to legal uncertainty and create loopholes. Moreover, I question a number of categorisation choices made and see a great number of still heavily criticised AI uses listed as medium and high risk, potentially further mainstreaming them.

Prohibited AI Practices

The AIA prohibits a limited number of AI practices that pose an unacceptable risk of harm to health, safety and fundamental rights. See our paper [AIA in-depth #2 | Prohibited AI Practices](#).

The first prohibition revolves around AI-driven manipulation but is limited to a narrow set of very rare practices. Here the AIA presents a grand opportunity to address the wider societal harms that AI-driven manipulation can bring and curb the trajectory towards the Internet-of-Minds.

The proposed prohibition of 'social scoring' is definitely a step in the right direction. The current wording however could leave the door open to a number of social scoring mechanisms that also deserve stricter scrutiny. We have seen many other instances of social scoring by public and private actors alike. While these do not consist of 'generalised' schemes of citizen scoring, examples of which we have seen in China, they do consist of the scoring of individuals for various purposes, such as social benefits fraud detection, loan or mortgage eligibility etc. For 'social scoring' to be effectively prohibited in Europe, the AIA should draw a clearer line between what is considered 'social scoring' and what can be considered an acceptable form of evaluation for a certain purpose.

Biometric identification for law enforcement

Under the current prohibition, many biometric recognition practices (a.o. biometric assessment (such as emotion recognition) and biometric categorisation, that both do not necessarily involve identification) remain allowed, also by law enforcement. For a thorough analysis of the ban on biometric identification, see our paper [AIA in-depth #2 | Prohibited AI Practices](#). In line with the EDPB, EDPS, EESC, many MEPs we recommend a ban on biometrics recognition (which includes biometric identification, but also all forms of 'emotion/behaviour/affect/intent/trait/gender/race recognition and categorisation with biometric recognition, which is now categorised as medium and high risk in some areas) both by private organisations and (semi-)public authorities. Exceptions for specific use cases (e.g. in healthcare) could be considered.

Additional prohibition: Indiscriminate tracking & profiling

The ubiquitous tracking of our entire behaviour through our online behaviour, our location data and our IoT data serves no obvious social benefit. While prohibiting these practices might be challenging, we believe that the further proliferation of these forms of widespread tracking of our entire lives by public and private actors should at least be curbed.

High Risk AI

Under the AIA, AI-systems that pose a risk of harm to health and safety or fundamental rights of persons, but nevertheless supposedly bring benefits to society, are to be considered high risk. Those AI systems will be allowed on the Union Internal market, as long as they comply with a set of mandatory requirements and follow conformity assessment procedures. This poses the risk of normalising and mainstreaming quite a number of AI practices that are still heavily criticised, often due to their lack of sufficient social benefit. See our paper [AIA in-depth #3a | High Risk AI Categorisation](#).

Secondly, this approach assumes that the risks high risk AI systems pose, also future ones, can be sufficiently mitigated by meeting the requirements of articles 9 through 15 AIA (which are (paraphrased: risk management system, datasets of high quality and data governance, documentation, transparency, human oversight, accuracy, cybersecurity and robustness). This is often not the case.

Under the current text, the assumption also is that (if in line with the AIA), AI could largely replace human decision making in law enforcement, the judiciary, enjoyment of essential services, migration and asylum, recruitment, hiring, firing and worker-assessment, education, democratic processes. Most AI is however technically incapable of making these decisions at a human level and it is questionable if it is even desirable. Ultimately, not all decisions can or should be simplified to 'ones and zero's'. We recommend to have certain decisions remain the ultimate prerogative of humans. See our paper [AIA in-depth #3b | High Risk AI Requirements](#). As regards the environmental impact of AI systems, the High Level Expert Group on AI holds a specific requirement to this effect, which we propose to add to the AIA, along with all other 'missing requirements' (see my answer to question 4).

3) **To what extent will the AI regulation affect Europe's competitiveness compared to the rest of the world?**

The AIA will strengthen Europe's competitiveness compared to the rest of the world. It is a widely advocated assumption that regulation stifles innovation and lowers Europe's competitiveness. There are several reasons as to why this assumption fails.

First and foremost, regulation gives clarity, legal certainty and guidance. Many private organisations have called upon the EU to provide this clarity, certainty and guidance, in particular SME's. Secondly, regulation creates a level playing field, ensuring that all actors are held to the same standards. Third, the argument that while the EU regulates the rest of the world innovates fails, because 'the rest of the world has to abide by the AIA, if it wants to introduce its AI systems on the EU internal market, the second largest economic area of the world. Fourth, we already see signs of the so-called 'Brussels Effect', where European laws set the standard for regulatory efforts around the world (e.g. the US and Japan). Fifth, it is well known that regulation generally serves as a 'stepping stone' for innovation. The AIA in particular, due to its granularity and step-by-step approach, can even serve as a tool to raise the quality, safety and trustworthiness of AI and as such drive high quality AI innovation, which raises Europe's competitiveness compared to the rest of the world. Sixth, it is not the first time that potentially harmful products or practices are being regulated, in order to protect citizens and the environment, such as REACH (hazardous substances).

4) **Can the AI regulation as drafted prevent discrimination against, for example, women or people of colour? Where is there perhaps room for improvement?**

The AIA's objective is to protect health, safety and fundamental rights against the potential ill effects of AI. It builds on the Ethics Guidelines for Trustworthy AI, drafted by the EU High Level Expert Group on AI, which are grounded in our fundamental rights. The right to non-discrimination is one of the fundamental rights enshrined in both the European Charter of Fundamental Rights and the European Convention on Human Rights.

The AI Act aims to protect this right in two main ways:

- It prohibits certain AI practices that present an unacceptable risk of harm to the right of non-discrimination (and other fundamental rights).
- It sets mandatory requirements for AI systems that pose a high risk of harm to health and safety or fundamental rights of persons (such as the right to non-discrimination), but nevertheless provide sufficient benefit to society.

As described in my answer to question 1), the prohibitions cover a limited set of AI practices (manipulation and exploitation, social scoring and biometric identification in law enforcement). The right to discrimination is particularly vulnerable when it comes to these practices. Thorough reading of the prohibitions however shows that they still leave ample room for discriminatory manipulation and exploitation, social scoring and biometrics recognition practices. In our paper [AIA in-depth #2 | Prohibited AI Practices](#), we make suggestions to amend the prohibitions in order to improve the protection of the right to non-discrimination (and other fundamental rights).

As described under 2), the categorisation choices made for high risk AI poses the risk of normalising and mainstreaming quite a number of AI practices that are still heavily criticised, not only due to their lack of social benefits, but also to their risk of bias, that can harm to the right to non-discrimination. To address this, propose to move a number of standalone AI-systems and practices listed in ANNEX III to the prohibitions:

- Biometric identification (one-to-many), categorisation and assessment
- Certain AI(-driven) decisions in employment, e.g. on hiring and termination
- AI determining or predicting the lawful use of public services (e.g. social benefits fraud risk prediction)
- Predictive policing, criminal profiling and biometric lie detection in law enforcement, criminal justice and asylum, migration and border control
- AI used for vote counting in elections
- AI to take judicial decisions

I welcome the alignment of the the requirements for high risk AI with the 7 requirements of the [Ethics Guidelines for Trustworthy AI](#), however, five requirements of the Ethics Guidelines are however not specifically or entirely dealt with in the AIA namely: (i) human agency (ii) privacy (iii) diversity, non-discrimination and fairness, (iv) explainability and (v) environmental and social well being. This is a missed opportunity, in particular because many of the risks AI poses are those of privacy, bias and discrimination, exclusion, inexplicability of the outcomes of AI decisions, the undermining of human agency and the environment, and are all reflected in our fundamental rights.

While some of these missing requirements are (partially) dealt with in existing legislation such as the GDPR (privacy and explainability) and the European Charter on Fundamental rights (non-discrimination), this is not sufficient. Moreover, by adding the missing requirements, the AIA can bring many human rights protections into the private sphere as well.

What is more important is that the AIA works from the premise that the requirements for high risk AI will sufficiently mitigate the risks of harm to health, safety and fundamental rights. This is however expected not to be the case in all circumstances. For discriminatory outcomes for example, it overlooks the fact that AI biases are not just the result of low-quality data, lack of human oversight or inaccuracy. The design of any artefact is in itself an accumulation of choices that can cause biases to creep in. And even with high quality data, documentation, human oversight, accuracy, robustness and cybersecurity, AI can still pose risks, particularly to the right of non-discrimination. Merely focussing on technical and procedural solutions does always not suffice to avoid this. Rather the socio-technical processes around AI need to be organised in such a way that that any discriminatory, unfair or otherwise harmful outcome of AI can be adequately identified and addressed.

I note that the (temporary) exemption of EU border information systems causes concern to the right to non-discrimination, as 'border control AI' has shown to largely impact vulnerable groups such as asylum seekers, many of which are people of colour.

As a minimum, I propose to add the 'missing' requirements from the [Ethics Guidelines for Trustworthy AI](#) to the requirements of Chapter 2 of Title III of the AIA:

- Human Agency (part of EGTAI requirement "Human Agency and Oversight")
- Privacy (part of EGTAI requirement "Privacy and Data Governance")
- **Diversity, Non-discrimination and Fairness**
- Explainability and better Transparency
- Societal and Environmental Well-being

Finally, the AIA is unclear as regards the situation where the requirements for high risk AI are not met. Art. 67 of the AIA deals with "compliant AI systems which present a risk", but only after these systems have entered the market. The potential gravity of the adverse effects of high risk AI, justifies a precautionary approach, rather than a post-hoc 'reparatory' approach.

5) Are the rules enshrined in the GDPR and the draft regulation adequate with respect to the rights of those affected by AI decisions to access information and appeal? And how can the people affected be made aware of those rights?

No, the AIA only holds transparency obligations towards natural persons for the following AI systems:

- AI systems intended to interact with natural persons (think of chatbots)
- AI systems used for biometric categorisation or emotion recognition
- AI systems that generate 'deep fakes' (audio, video, image)

The AIA does not hold any rights (access to information, right to explanation, right to complain, right to redress, etc.) for 'affectees' of AI-systems' outcomes or decisions, nor does it define 'affectees' in any way.

Moreover, while the GDPR offers some frameworks for the right to an explanation of AI decisions (in the recitals) and the right to human intervention. These frameworks are insufficient to ensure adequate explainability of AI decisions. The right to human intervention in the GDPR for example only exists in the event of a fully automated decision, which has led to numerous court cases on the questions what is to be considered 'meaningful human intervention'. Moreover, the GDPR deals with situations where personal data is involved and it is well known that a decision based on non-personal data can also have a major impact.

There have been multiple calls to improve the AIA on this point, and include specific rights for 'affectees' of AI-systems' outcomes, including automated decisions. In order for affectees to be able to exercise these rights however, they need to be aware not only of the existence of such rights, but also of the fact that they were affected by an AI-system. This requires a broader notion of 'transparency' than merely the one described above. Here we again refer to the Ethics Guidelines for Trustworthy AI, which holds this broader notion of transparency (including explainability) and which should be added to the requirements for high risk AI.

6) How reliable is a compliance assessment for a high-risk application that has been conducted by providers themselves? Do we need external evaluation, particularly in sensitive areas?

The AIA contains a complex accountability structure with a lot of text on third party conformity assessment by notified bodies, while only biometric recognition and categorisation outside law enforcement is subject to third party prior conformity assessment. Prior conformity of all other standalone high risk AI on ANNEX III are self-assessed.

The complexity of the AIA and the requirements in combination with self-assessment runs the risk of this process simplifying being reduced to check lists where a simple 'yes' or 'no' could suffice to meet the requirements. This would make the AIA fail to achieve its initial objectives of promoting and driving innovation of AI that is trustworthy and in line with our fundamental rights and societal values. I recommend to have all high-risk AI be third-party assessed.

7) Do you see any significant terminological ambiguities in the AI regulation, and, if yes:

- what regulatory complications may arise from them;
- and how might such complications be avoided or remedied?

Our first [in-depth analyses of the main parts of the AIA](#) (objective, scope, definition, prohibited AI practices, high risk AI classification and requirements, including the accompanying ANNEXES (I, II and III), have not shown major terminological ambiguities within the AIA itself as yet. I do however note that the multitude of various actors and their different obligations (providers, users, distributors, importers) cause confusion as to who is responsible for what exactly. Also, the lack of any definition of the party or parties affected by the AI systems' outcomes causes concern, especially whereas these parties are usually referred to as 'users' in other EU regulations and directives.

I also caution against sub-defining AI-systems in the AIA (definitions for Open Source AI and General Purpose AI have been proposed) as this could lead to legal uncertainty and create loopholes.

- 8) According to a recent survey by Bitcoin, 49% of businesses asked saw legal uncertainty as an obstacle to the introduction of AI applications. Will the AI regulation improve that situation, in your opinion, or might it even exacerbate it, particularly for SMEs?

The AIA will bring legal certainty, a level playing field and innovative guidance, particularly for SMEs. Nevertheless, a serious (financial) effort should be made to aid SMEs in understanding and following the rules of the AIA. See also my answer to question 3).

- 9) The Federal Government has made it clear that it wishes to enshrine rules for AI applications for security agencies separately from the main text. Do you think this makes sense, and what are the advantages and disadvantages of separate regulation?

I advise against this. First and foremost, there is no commonly accepted definition of (national) security. The Article 29 Working Party at the time called upon the Council, the Commission and the Parliament to come to an agreement in order to define the principle of national security and be conclusive as to what should be regarded as the exclusive domain of the Member States. As far as I know, no such definition exists to date.

There is however a more fundamental question to be asked as regards the exclusion of national security from the scope of the AIA. I assume that the Federal Government refers to art. 4(2) of the TEU to motivate the separation. This article states that national security is the sole competence of the Member States, which means that the EU has no competence in regulation matters of national security. The AIA however does not specifically regulate national security matters. It is a broad product regulation, aimed at protection of health, safety and fundamental rights. The exclusion of national security from the scope of the AIA could lead to the exclusive competence of Member States to regulate AI (or not) in the area of national security. The EU and Member States' competences are however already defined in the Treaties of the EU, and any changes or additions to those cannot be made by simply excluding certain areas from EU regulation. Such an approach would undermine the workings of the Treaties and even conflict with the principle of sincere cooperation of art. 4(3) of the TEU, stating that Member States should refrain from taking any action – including legislative – that could jeopardise the attainment of the Union's objectives.[1]

If one were to allow such an exclusion for AI legislation, one could argue excluding national security from any and all EU legislation that (even remotely) has a link with national security. Think of the (proposed) NIS Directive, ECI Directive and REACH[2], but also EU legislation related to motor vehicles. As much as we do not (have to) exclude national security from such legislation, we should not exclude it from the AIA.

- 10) To what extent does the AI regulation enable members of the public to recognise and understand the use of AI systems and to make use of their rights if they are affected by AI-powered decisions or preparations for decisions, and are the transparency requirements arising from the first sentence of Article 52 sufficient to inform them that AI systems automatically or semi-automatically make, prepare or influence decisions?

It does not. The transparency requirement for high risk AI only applies in the relationship between 'AI providers and AI users (organisations that deploy AI systems they have not built themselves, but have obtained from other parties)' and not towards members of the public.

Art. 52 paragraph 1 is aimed at AI-systems that interact with natural persons, e.g. chatbots. It does not hold any obligation to inform natural persons that AI systems automatically or semi-automatically make, prepare or influence decisions. See also my answer to question 5).

- 11) With regard to large data sets for public-interest/research data, to the best of your knowledge, can research sandboxes be designed in such a way that no structural impingement of data protection can occur as a result of the use of research data (example: European Health Data Space)? If yes, how, and if no, could you please elaborate on the reasons?

There have been several proposals to exclude of AI (including datasets) used solely for research and (commercial) development from the scope of the AIA. This raises some serious concerns.

[1] Rojszczak (2021) "The uncertain future of data retention laws in the EU: Is a legislative reset possible?"

[2] See ENISA: <https://www.enisa.europa.eu/topics/threat-risk-management/current-risk/laws-regulation/national-security>

AI does not tend to 'stay' in the lab. Research in the field of AI is often open-access and open-source as codes are shared and uploaded to platforms such as GitHub, which is accessible and free to use. This gives anyone the opportunity to use new AI techniques and codes for any purpose or practice, also high risk ones, the latter possibly without any adherence to the requirements for high risk AI. Any 'downstream' user would have to make sure the high risk AI system is in line with the AIA, but this is almost in all cases merely a self-assessment obligation.

[3] [Guidance in a Nutshell - SR&D and PPORD: https://echa.europa.eu/documents/10162/2324906/nutshell_srd_ppord_en.pdf/14675e6c-b2cf-4049-81ad-3d1bc41ace6d"]

I worry that such exclusion could lead to a declining incentive to approach AI research in a multidisciplinary manner, where multiple domains, such as ethics, law, social sciences, political sciences, psychology, medicine, education, media, communication and the humanities are involved.

I also however fully respect the freedom of research. But such freedom is not absolute. Moreover, the issue at hand is not new. Also, here we can draw inspiration from existing legislation such as REACH, which holds specific arrangements for when hazardous material is used for Scientific Research and Development.[3]

In the same spirit, I recommend that rather than fully excluding scientific research and development from the AIA, specific arrangements are included to facilitate it. Such arrangements could first and foremost include a definition of "Scientific Research and Development" along the lines of the definition in REACH. See our paper [AIA in-depth #1 | Objective, Scope, Definition](#). As a next step, obligations and/or exemptions could be added to Chapter 3 specifically aimed at scientific research and development.

- 12) Have the social effects of AI been adequately researched or is there a need for a specific research ethic and structural scientific research/evaluation to critically investigate examples of applications, e.g. from the field of security technology, and ensure that AI does not discriminate and cement inequality?**

No. AI systems are part of complex socio-technical systems through which they can affect society, and it is still unpredictable how AI will affect society in a certain scenario. This also means that it is hard to develop research/evaluation methods that are adaptable assess every scenario and address each ethical or societal impact. While there are many research initiatives, this particular type of research is still at its infancy and growing slowly in comparison to the fast development and application of AI. To keep up to pace, more research is urgently need, especially in areas of security and fairness. Moreover, as AI impacts virtually all aspects of our society, AI research should adopt a truly multidisciplinary approach, involving scientists from a variety of fields, such as ethics, law, social sciences, political sciences, psychology, medicine, education, media, communication and the humanities.

- 13) On what points do you still see the need for improvements in the compromise proposals put forward by the Czech Presidency of the Council on 15 July 2022 as far as the definition of AI, the identification of high risk systems and the classification of AI applications in Annex III are concerned?**

The new definition proposed by the Czech Presidency in its latest compromise proposal of 16 September 2022 is an important improvement. It no longer refers to ANNEX I, which I fully support. It also focusses on the characteristics, or properties of a system, that are relevant to be regulated, rather than certain AI-techniques, which avoids circumvention.

This latest proposal however also deletes several crucial high risk AI systems/uses, some of which previously added by the French Presidency, which is problematic and should not be adopted. Among them are AI systems used for environmental protection and emissions, crime analytics, verification of travel documents.

- 14) **Does the AI regulation, in your view, provide sufficient room for manoeuvre for German and European AI research to compete with the research conditions in the US and China, and which provisions, if any, of the AI regulation might, especially in respect of the proposed rules for sandboxes, have a limiting effect on future AI research projects as well as on technology transfer from research to products licensed for the market?**

Yes, see also my answer to question 3).

- 15) **How, in your view, can uniform interpretation of the AI Act in all EU member states be achieved?**

The AIA is an EU regulation that aims to ensure the uniform application of AI rules across the EU. Interpretation of the AIA by all relevant parties requires awareness, knowledge and guidance, including the proper (financial) incentives to effectuate such, in particular with the general public, micro and small-, medium and large enterprises, policy makers, public organisations, law enforcement, the judiciary, educators, social partners and researchers.

- 16) **What should governance in the context of supervision and scrutiny of AI applications look like, in your opinion, specifically in terms of the set-up of the European AI Board, its cooperation with national authorities, and the distribution of responsibilities between it and national authorities, and what criteria should, in your opinion, be applied for the selection of national authorities?**

The governance structure in the AIA is quite elaborate and complex. It should be noted that supervisory structures vary from Member State to Member State. Some have multiple supervisory authorities that could have a role under the AIA, while others have only a few supervisory authorities. Both situations could lead to complications. The involvement of many supervisory authorities could render the supervisory activities complex, scattered and difficult to manage. The involvement of only a few (or a single) supervisory authorities/y could render the supervisory activities ineffective.

As regards the AI Board I recommend to include representatives from wider society, including the social partners and NGO's in the AI Board. I further strongly recommend to include expert advisors on AI, data science, the law, ethics, social sciences, psychology, economics, labour relations, healthcare and education in the AI Board.

- 17) **Would it make sense, in your view, to add a separate "norms and standards" part to the planned regulation? After all, the standardisation of technologies that are in the throes of creation and/or growth is a crucial factor in the commercial viability of specific solutions and thus on the market prospects of individual providers both current and future. Should the Commission see its duty in vigorously defending the (standardisation) interests of German and European players in the field of artificial intelligence in the relevant international bodies?**

The European Commission has already issued a request for standardisation of the requirements for high risk AI to CEN-CENELEC. Standardisation processes are however heavily industry dominated, due to the lack of access to standardisation bodies for other stakeholders or the lack of financial capacity to participate in standardisation activities that do allow other stakeholders. Given the broad and deep impact of AI on all aspects of society, I strongly advocate for a revision of the EU Standardisation Regulation of 2012 so as to facilitate participation of other relevant stakeholders from academia, SME's, civil society and NGOs in standardisation activities.

- 18) **Would it make sense, in your opinion, for the AI regulation to classify potential AI solutions not only defensively into categories of risk but also, complementarily, into categories of opportunity or merit? Would this not be a way to emphasise the enormous innovative and creative potential of AI in a highly dynamic market, which, unlike in the US and China, happens too rarely and too tentatively in Germany and the EU?**

I applaud the idea of emphasising AI opportunities and merit, but I do not think that the AIA is the right place for that.



ABOUT ALLAI

ALLAI is an independent organisation that aims to foster, promote and achieve the responsible development, deployment and use of AI.

ALLAI's mission is to take a holistic approach to AI, taking into account all impact domains such as economics, ethics, privacy, laws, safety, labour, education, etc. ALLAI aims to involve all stakeholders in its mission: policy-makers, industry, social partners, consumers, NGOs, educational and care institutions, academics from various disciplines.

ALLAI was founded by the three Dutch members of the High Level Expert Group on AI, Cateljine Muller, LL.M., Prof. Virginia Dignum and Prof. Aimee van Wynsberghe.

ALLAI refers to Stichting ALLAI Nederland, a foundation under Dutch Law. No entity or person connected to ALLAI, including its Board Members, Advisory Board Members, employees, experts, volunteers and agents, is responsible or liable for any direct or indirect loss or damage suffered by any person or entity relying wholly or partially on this communication.

CONTACT



ALLAI
Prinseneiland 23A
1013 LL Amsterdam
The Netherlands



www.allai.nl
[@ALLAI_EU](https://twitter.com/ALLAI_EU)
welkom@allai.nl

