Meijers Committee

CM2203 Comments on the AI Regulation Proposal

1. Introduction

Considering the fast development of AI technologies and the impact AI can have on individuals and the protection of their fundamental rights, the AI proposal of the European Commission (the AI Act) is an important initiative that is to be welcomed.[1] The impact of AI-based procedures and goods include not only the fundamental rights to privacy and data protection but also the right to non-discrimination, children's rights, the rights of suspected persons and their right to a fair trial, and more generally, the right to effective judicial protection.[2]

However, the current proposal fails to provide adequate protection for citizens. The Meijers Committee is concerned that the provision of prohibited AI systems will only pay lip service to the goal of protecting fundamental rights and preventing discrimination and stigmatization of particular groups.[3] The AI Act should ensure the protection of individuals against possible harm caused by AI technologies. It should provide procedural guarantees and access to legal remedies. Further, it should identify the actors who can be held accountable for potential damages and for the violation of rights.

In this comment, while considering the amendments in the Presidency compromise text of 29 November 2021,[4] the Meijers Committee addresses specific gaps in protection in the AI proposal and provides some suggestions for improvement.

Aside from the more detailed recommendations in the comments below, the Meijers Committee proposes to:

- Include individual safeguards to ensure transparency and accountability of the use of AI systems;
- Expand the scope of the AI Act to databases in the field of migration and asylum law;
- Prohibit the use of polygraphs, lie detectors, and social scoring systems.

2. AI Act as a minimum level of protection

As a preliminary remark, the Meijers Committee notes that several provisions and the explanatory memorandum to the AI Act proposal include minimum standards

[1] 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, COM/2021/206 final.
[2] See also the Council of Europe's recommendation on the human rights impacts of algorithmic systems and the proposals it includes for emphasizing the positive effects but preventing and mitigating the potential adverse effects of AI technologies, CM/Rec (2020), 8 April 2020.
[3] See also European Data Protection Board & European Data Protection Supervisor *Joint Opinion 5/2021 on the Artificial Intelligence Act*, 18 June 2021, p. 11.
[4] Council document 14278/21, 29 November 2021.

and safeguards. The Meijers Committee recommends explicitly providing the AI Act only offers minimal protection and is without prejudice to more favourable provisions. This will ensure that national authorities and private actors will not use the AI act to lower their existing protection.

3. The necessity of including specific individual safeguards: accountability

The AI Act addresses providers and users of AI systems. However, the AI Act does not create individual rights for persons affected by AI systems. Consequently, individuals do not have a right to redress under the AI Act. Individuals require such a right when they are wrongfully submitted to prohibited AI practices, such as social scoring or biometric identification systems, or suffer harm when providers or users of AI systems have not met their obligations under the AI Act.[5]

The Meijers Committee recommends including a right to lodge a complaint with a competent national authority established or designated under Article 59 of the AI Act.[6] Furthermore, the AI Act should include a right to an effective judicial remedy against a provider or user of an AI system where an individual considers that an infringement of the AI Act has harmed this person.

Additionally, any person who has suffered material or non-material damage due to an infringement of the AI Act should have the right to receive compensation from the provider or user of an AI system. For this purpose, the AI Act should also clearly provide that any provider or user of an AI system is liable for the damage caused by the use of an AI system that infringes the AI Act. In this case, the AI Act should guarantee a low threshold for individuals to start legal remedies, ensuring that such procedures are not hampered by the question of which authority or private actor is accountable. This means that there should be no lack of transparency or doubt on which organization or public authority is to be held accountable for any harm or violation of fundamental rights connected to the use of AI. The AI Act should therefore provide in the obligation for public and private organizations using an AI-based tool or product to identify, before this use, which entity or organization is to be held accountable for possible harm or fundamental rights violations. This allows the person whose rights or interests are impaired to address this entity or organization directly.

4. Access to effective judicial protection: transparency of AI-based tools

In the context of AI, sufficient guarantees to ensure the individual right to effective judicial protection, as included in Article 47 of the Charter on Fundamental Rights (CFR), are indispensable. The Meijers Committee calls upon the EU legislator to ensure that national courts and tribunals have sufficient powers and tools to provide effective remedies for individuals. This also means that individuals affected by the

[5] Alexandru Circiumaru, 'Three proposals to strengthen the EU Artificial Intelligence Act', *Ada Lovelace Institute*, 13 December 2021, https://www.adalovelaceinstitute.org/blog/three-proposals-strengthen-eu-artificial-intelligence-act/.
[6] See similarly, BEUC, 'Regulating AI to protect the consumer: Position paper on the AI Act', 2021, https://www.beuc.eu/publications/beuc-x-2021-088_regulating_ai_to_protect_the_consumer.pdf.

application of AI-based tools or goods must have the possibility to address possible flaws in the architecture or development of the AI technologies. The necessity of informed decision-making has, albeit in a different context, underlined as being 'able to ascertain the reasons upon which the decision taken in relation to him or her is based, either by reading the decision itself, or by requesting and obtaining notification of those reasons.'[7] Therefore, the Meijers Committee proposes the inclusion of specific provisions ensuring the right to information on the development and use of AI, access to information on the development, content and criteria used in an AI-based tool, procedure or scoring system.

We emphasize that AI-based tools or procedures which do not necessarily involve the processing of personal data and are therefore not covered by the GDPR may still impair individual rights. Possible examples are AI-based products, such as self-driving cars, or AI-based public services, such as automatically opening bridges, which may cause individual harm also without processing personal data. Therefore, the AI Act should include, complementary to the GDPR, specific procedural rights and remedies, including the right for repair and financial compensation.

4. Relationship with 'prohibited automated decision-making' in Article 22 GDPR

Addressing the protection of individuals, the Meijers Committee questions how the prohibition of social scoring systems interacts with Article 22 GDPR. This provision gives individuals the right not to be subject to automated decision-making if the decision produces legal effects concerning them or significantly affects them. If a social scoring system does not lead to detrimental or unfavourable treatment, it is questionable whether individuals still have recourse to Article 22 GDPR. The Meijers Committee recommends that the AI Act clarifies the relationship between the criteria for the application of Article 5(1)(c) AI Act (namely: detrimental or unfavourable treatment) and the criteria for the application of article 22 GDPR (namely: legal effect or similarly significant effect).

5. Limited scope of the AI Act

Exclusion of intelligence and national security agencies
The Meijers Committee notes that Article 3(40) in the current proposal defines law enforcement authorities as 'any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'. While this definition excludes national security and intelligence agencies, it should be noted that in some Member States, the distinction between law enforcement and public order on the one hand, and national security on the other, is not so clear. In some countries, one organization may perform tasks in both fields. In such cases, the AI Act should clarify that the minimum safeguards as defined based on the AI Act are also applicable to these law enforcement

[7] See CJEU, joined cases *R.N.N.S and K.A.* C-225/19 and C-226/19, point 36.

authorities when they act for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. This also includes safeguarding against and the preventing threats to public security.

Exclusion of large-scale databases on third-country nationals
Article 83 of the AI Act excludes already existing large-scale databases listed in Annex IX (SIS, VIS, Eurodac, ETIAS, EES, ECRIS-TCN and the interoperability proposal) from the scope of the AI proposal. The Meijers Committee is concerned about the impact of this exclusion on the fundamental rights of third-country nationals whose data are reported in one of these systems. The Meijers Committee notes that the current proposal lacks justification for this exclusion.

Many AI-driven systems and large-scale databases are already in place. The risks for adverse effects on fundamental rights, specifically the right to non-discrimination, that these systems and databases entail, have been well documented by among others, the Fundamental Rights Agency (FRA),[8] the European Data Protection Supervisor[9] and rapporteurs from the United Nations.[10] The Meijers Committee calls upon the EU legislator to clarify why the systems mentioned above and databases are outside the scope of the AI Act.

6. High-risk systems and narrow definition of 'persons in a vulnerable situation'

Under Article 7 of the AI Act, the Commission can update the list in Annex III on high-risk systems, taking into account, amongst others: the extent to which potentially harmed or adversely impacted persons are in a vulnerable position in relation to the user of an AI system, in particular due to an imbalance of power, knowledge, economic or social circumstances, or age (Article 7(2) (f)).

The Meijers Committee considers that the definition of vulnerability within the context of 'high-risk systems' as currently included in the proposal is insufficient to protect individuals against possible harms of AI-based tools or decision-making. First, this definition is too narrow, not considering asylum seekers recognized as a vulnerable group in EU law or national and ethnic minorities, such as Roma. Therefore, the EU legislator should extend the definition of vulnerability by adding 'in particular due to..., status, nationality or ethnic minority'.

Second, Article 5(1)(b) prohibits AI systems that exploit vulnerabilities of a specific group of persons due to their 'age, physical or mental disability'. This is a limited view on what makes someone vulnerable and susceptible to manipulation. For instance, people living in poverty are more susceptible to predatory lending

[8] FRA, *Big Data: Discrimination in data-supported decision making*, 2018.
[9] EDPS, Opinion 4/18 on interoperability between EU large-scale information systems, 2018.
[10] UN Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, *Racial discrimination and emerging digital technologies: a human rights analysis*, 2020.

advertised to them with personalized ads. Therefore, the Meijers Committee supports the addition in the provision mentioned above of vulnerable persons 'due to their social or economic background', as proposed in the Presidency compromise text of 29 November 2021.

7.Concern about the proposed use of polygraphs or lie-detectors

The AI Act explicitly allows for the development and employment of 'polygraphs and similar tools or to detect the emotional state of a natural person' as examples of AI systems intended to be used by first, law enforcement authorities and second, for migration, asylum and border control management.[11]

The Meijers Committee notes that this use of 'AI' entails severe risks for protecting fundamental rights, resulting in stigmatising certain groups or individuals (including suspected but not convicted persons, third-country nationals, and asylum seekers). Furthermore, scientific evidence for the reliability of lie-detectors or polygraphs is lacking. Experts have emphasized the serious fundamental rights impact and flaws and ethical problems of using such methods.[12] Within fundamental rights law, the EU legislator and individual Member States have a special responsibility when allowing or introducing new technologies. This responsibility also involves the obligation of ensuring that possible or future use of AI technologies does not have a chilling effect for individuals, limiting their right to private life and their freedoms of thought, expression, and religion.[13] Therefore, the Meijers Committee calls for an absolute prohibition of polygraphs or any tools to detect the emotional state of natural persons in the fields as mentioned earlier of law enforcement and migration, asylum and border management, or in any other field in which the use of such technologies can damage the integrity and human rights of individual.

Furthermore, the AI Act should clarify that facial recognition systems in public areas are prohibited, as submitted by the European Data Protection Board and the European Data Protection Supervisor.[14] The Meijers Committee supports the concerns as expressed by the European Parliament in the resolution on the use of AI for law enforcement purposes and EU funded projects such as iBorderctrl, allowing for the use of lie-detectors.[15]

8. Prohibited use of social scoring systems

[11] See point 5 and 6, in Annex III on 'high risk AI systems'.
[12] Javier Sanchez-Monedero & Lina Dencik (2020): The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl, *Information, Communication & Society*, DOI: 10.1080/1369118X.2020.1792530
[13] See ECtHR on the right to private life in Article 8 ECHR: *S. and Marper v. UK*, no. 30562/04 and 35606/04, para. 71 and with regard to the freedom of expression, Article 10 ECHR: *Goodwin v. UK* 27 March 1996, no. 17488/90, para. 39.
[14] https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en.
[15] See resolution P9_TA(2021)0405 point 31 and 32.

The Meijers Committee supports the general prohibition in the AI Act of AI-based social scoring for general purposes done by public authorities. The AI Act should ensure the banning of systems resulting in discrimination and stigmatization of specific individuals or groups of persons. The child benefits scandal in the Netherlands illustrated the detrimental effects of administrative tools based on biased and discriminatory risk models.[16] The development and use of these models resulted in the stigmatization and discrimination of particular groups of individuals, especially those with double nationality or (assumed) immigration backgrounds. Furthermore, individuals had no or few possibilities to rebut the trustworthiness of risk models in the decision-making. As underlined by the UN Rapporteur on Extreme Poverty and Human Rights in the SyRI case, which concerned the use of risk scoring systems by local governments in the Netherlands, those systems tend to specifically affect the most vulnerable groups of society including minorities or persons with a migration background.[17]

The Meijers Committee is concerned that Article 5 (1) (c) of the AI Act and the explanation on p. 13 does not provide sufficient safeguards to eliminate the potential disproportional and discriminatory use of social scores or risk models. According to this provision, 'the placing on the market, putting into service or use of AI systems by public authorities or on their behalf for the evaluation **or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score leading to either or both of the following:**

(i) **detrimental or unfavourable treatment** of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected;
(ii) **detrimental or unfavourable treatment** of certain natural persons or whole groups thereof that is **unjustified or disproportionate to their social behaviour or its gravity'** [emphasis by the Meijers Committee].

This text lacks clarity on what is meant by the phrases 'detrimental or unfavourable treatment' and 'unjustified or disproportionate'. The Meijers Committee submits that the AI Act should further specify those definitions. First, where paragraph (i) describes use 'unrelated to the contexts in which the data was originally generated or collected', the EU legislator should consider replacing that text with : 'unlawful use or use other than the legitimate purpose for which the data was originally generated or collected'. Second, in paragraph (ii), the EU legislator should consider removing the words 'to their social behaviour or its gravity' from the phrase 'that is unjustified or disproportionate to their social behaviour or its gravity'.

[16] See on the problems of the algorithmic enforcement in the Dutch child benefits scandal: https://eulawenforcement.com/?p=7941 and the letter of the Dutch government to the Dutch Parliament of 15 January 2021, *Kabinetsreactie rapport 'Ongekend Onrecht'* recognizing the discriminatory effects of the use of risk models at stake by the tax authorities, p. 14 ff.
[17] Philip Alston, Amicus Curiae in Syri case by UN Special Rapporteur on Extreme Poverty and Human Rights, 26 September 2019, www.ohchr.org/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf.

9. Prohibited AI systems and unclear definition of 'harm'

Article 5 of the AI Act defines AI practices that are generally prohibited because their use will cause or is 'likely to cause' to a person or any other person 'physical or psychological harm'. The EU legislator should extend the definition of 'harm' (and thus prohibited AI systems) to mechanisms that use results in violation of fundamental rights or any other harm, including legal and financial harm. In this regard, the legislator should clarify that a cumulation of (more minor) harms related to AI systems should be regarded as 'harm' within this context.

10. Transparency obligations – relationship with data protection rights

Article 52(2) of the proposed AI Act provides that providers must 'ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use.'

It is unclear what this provision adds to the already existing transparency requirements in the GDPR, including the obligation of providers to inform data subjects and the individual right to be notified and have access to data being processed. The Meijers Committee is concerned that this transparency provision in the AI Act may be read or applied as a limitation of the general GDPR provisions. The AI act should clarify that none of the provisions in the AI Act can be applied to limit the level of protection offered by the fundamental right to private life and data protection as protected in the EU Charter on Fundamental Rights and the GDPR.

11. Deep fake and exception to transparency

Article 52(3) of the AI Act includes an exception from the transparency obligation when the deep fake 'is necessary for the exercise of the right to freedom of expression'. The publication of a deep fake is generally an exercise of freedom of expression, since a deep fake is a communicative act.[18].

The exception for freedom of expression in general therefore conflicts with the entire provision. The Meijers Committee recommends limiting the exception to deep fakes used for 'journalistic purposes and the purposes of academic, artistic or literary expression', similarly to the exception in the GDPR.

12. Use of AI for military or national security purposes

The Council's Presidency text proposes to change Article 2 such that the regulation 'shall not apply to AI systems developed or used exclusively for military or national security purposes'. The text adds to recital 12: 'When AI systems are exclusively developed or used for national security purposes, they should also be excluded from the scope of the Regulation, taking into account the fact that national security

[18] Some deep fakes may not qualify as protected expression, e.g. when the deep fake contains hate speech

remains the sole responsibility of Member States in accordance with Article 4(2) TEU'.

Regulating the development of AI for military purposes by the public sector would raise issues with the competencies of the EU. However, the EU could regulate the development of AI for military purposes by the private sector. However, Article 2 in conjunction with recital 12 can be read as excluding both AI systems developed by the public and private sector from the scope of the AI Act when these systems will be used for national security purposes, as the provision does not differentiate between the public and private sectors. The Meijers Committee questions the rationale of excluding AI systems developed by the private sector when this is not required according to Article 4(2) TEU. In *La Quadrature du Net a.o.* and *Privacy International*, the CJEU has held that EU law applies to the activities of the private actors aiming to safeguard national security (in that context it concerned telecom services that retain and transmit metadata for intelligence services that work to protect national security.[19] The CJEU held that the e-Privacy Directive applies to such data retention and transmission despite Article 4(2) TEU). Article 4(2) does not require the legislator to exclude AI systems developed by the private sector for national security purposes from the scope of the Regulation.

The amended proposal of recital 12a in the Presidency Act clarifies that if AI systems are developed for military purposes but are also used for other purposes, this latter use will also fall within the scope of the AI Regulation. The Meijers Committee welcomes this amendment as, especially within the field of border and migration control, AI developed for military or security purposes could be used by national authorities or border agencies, including Frontex. The Meijers Committee calls upon the EU legislator improve the amendment by adding a parallel phrase that ensures that AI systems also fall within the scope of the AI Regulation if they are exclusively developed for national security but employed for other purposes including border and migration control.

13. Conclusion

The Meijers Committee hopes that the EU legislator will take the previous comments on board during the further negotiations on the AI Act. As always, we remain at your disposal to answer any questions or discuss possible amendments to the proposal.

[19] CJEU *Quadrature du Net*, C-511/18 and C-512/18 and CJEU *Privacy International*, C-623/17.