BEUC The European Consumer Organisation

AI Act – BEUC's preliminary assessment

DISCLAIMER: this document is BEUC's preliminary assessment of the AI Act. A fully fledged position paper will be published soon.

On 21st April 2021, the European Commission published a proposal for a Regulation laying down harmonised rules on artificial intelligence ('Artificial Intelligence Act').

AI has the potential to bring many positive things for consumers. It can power new products and services and help make consumers' lives easier and more convenient. For example, banks use AI to track suspicious activities and prevent fraud; public authorities use it to process and answer citizen requests; smart phones integrate virtual personal assistants that resort to AI; and social media applications use AI to organise, moderate and personalise their content feeds.

However, AI also comes with significant risks and challenges for consumers. For example, there is a risk of bias and unfair discrimination among different groups of people on the basis of economic criteria, gender or a person's health. More broadly, the use of AI can negatively affect consumers' autonomy and freedom of choice.[1]

We welcome that the European Commission has put forward a legal instrument aimed at regulating AI.

We strongly regret, however, that the AI Act proposal generally fails to address consumers' main concerns and expectations. This is particularly due to its narrow scope, focused on so-called "high risk AI" applications, and the fact that the need to strengthen consumers' rights is neglected. Moreover, the proposal relies heavily on industry's own unvetted assesment of compliance with the legislation and does not set up a sufficiently strong governance and public and private enforcement system. Finally, the methodology used to list specific AI systems within the scope of application of regulated AI systems does not seem to be sufficiently future-proof.

We hope that the EU's co-legislators (i.e., the European Parliament and the EU Member States) will address these shortcomings and improve the proposal so that it provides the rights and protections that consumers need while enabling the path for innovation that respects our fundamental values.

Below are some preliminary recommendations to address key issues of the proposal from a consumer perspective.

[1] You can find more information about consumer perceptions about AI in this survey: https://www.beuc.eu/publications/beuc-x-2020-078_artificial_intelligence_what_consumers_say_report.pdf

1. The prohibited AI practices need to be clarified and strengthened

Article 5 of the proposal establishes a list of four AI practices that should be banned.

BEUC strongly welcomes this regulatory approach. Certain AI practices represent such an important risk for consumer rights, fundamental rights and our societal values that the most adequate regulatory solution is a clear prohibition.

However, several elements need to be improved to better take into account consumers' interests and ensure a broad and clear application of these rules:

- Art. 5 (1) a) is limited to AI that is used intentionally to materially distort behaviour, causing physical or psychological harm to someone. Yet, AI that manipulates, discriminates, misleads or otherwise harms consumers in a manner that causes *economic* and *societal* harm is not covered. These harms should also be included.

- Some terms used in this Article need to be modified as they would effectively limit the scope of this provision too much (e.g., it should cover any "technique", be it subliminal or not).

- Art. 5 (1) b) is limited to AI that exploits the vulnerabilities of specific groups such as children or mentally disabled persons, with the specific intention to materially distort their behaviour leading to physical or physiological harm. While ensuring protection to the most vulnerable groups, this provision does not take into account the constant state of vulnerability of all individuals created by exposure to "black box" technology and economic practices and consequences that consumers cannot grasp. There is a structural and architectural unbalance ('digital asymmetry'[2]) that should be addressed in the formulation of Article 5.

- In Arts. 5 (1) a) and b), the wording "*in order to*" limits the application of this provision to AI whose 'intended use' is to cause physical or psychological harm, thus excluding the 'potential use' or 'foreseeable use' of the AI.[3] We strongly reject the requirement to prove intent which is not required under EU consumer law in case of unfair commercial practices and would be a significant and inacceptable step backwards with regards to the level of protection that consumers need and are entitled to expect under EU law. If not changed, it would also mean that these provisions are in practice non-enforceable.

- Whereas the use of social scoring by public authorities is prohibited, which is welcome, its use by private entities, and thus commercial uses, is not regulated adequately by the AI Act.[4] This highly problematic gap must be addressed. In this regard, it must be noted that the European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS)[5] are requesting a ban on any type of social scoring.

[2] https://www.beuc.eu/publications/beuc-x-2021-018_eu_consumer_protection.0_0.pdf, at 46 et seq.

[3] See Recital 16 of the proposal;

[4] We can envisage certain types of social scoring used by private bodies being regulated as high-risk AI (e.g. Annex III – Points 3 and 4);

[5] https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en

- Remote biometric identification systems (Art. 5 (1) d))[6]:
  - Under the current proposal, the use of real-time remote biometric identification systems (e.g. facial recognition AI) in publicly accessible spaces[7] for the purpose of law enforcement would be prohibited but several exceptions are foreseen.
  - The use of real-time and post remote biometric identification systems by private entities are only classified as high-risk AI and thus permitted (Annex III – Point 1).
  - Due to its intrusiveness and the risk it represents for fundamental rights and core democratic principles, the use of remote biometric identification systems by private entities in public spaces should be regulated as strictly as any other use. In this sense, several organisations, regulatory authorities and policy makers[8] are already requesting a blanket ban on the use of this technology. If, nevertheless, certain exceptions are envisaged for public entities, such exceptions must be accompanied by specific safeguards to guarantee the respect of the necessary, proportionality and fairness principles as well as fundamental rights.
- AI used to identify emotion recognition is either classified as high-risk AI (if used by public bodies for law enforcement purposes)[9] or subject to weak transparency obligations (if used by private actors).[10] This is not sufficient. Researchers have demonstrated that "*it is not possible to confidently infer happiness from a smile, anger from a scowl, or sadness from a frown, as much of current technology tries to do when applying what are mistakenly believed to be the scientific facts*".[11] The use of emotion recognition systems should be more strictly regulated and only permitted in very specific cases.[12]

2. The proposal needs to regulate all AI and not only high-risk AI.

The scope of the proposal is too limited and is not future-proof:

First, it has a strong focus on 'high-risk AI', thus almost completely excluding from the rules applications to be considered low- and medium- risk. Only Art. 5 (prohibited practices) and Art. 52 (transparency measures for certain AI) reach beyond 'high-risk' AI.

As a consequence, we can envisage that a lot of AI applications that consumers use in their everyday lives and that can have an important impact on consumers and on our societies

[6] '*remote biometric identification system*' means an AI system for the purpose of identifying natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified (Art. 3 (36) of the proposal);

[7] '*publicly accessible space*' means any physical place accessible to the public, regardless of whether certain conditions for access may apply (Art. 3 (39) of the proposal);

[8] E.g. See footnote 6 and https://reclaimyourface.eu/;

[9] See Annex III – Point 6, b);

[10] AI used by public authorities for emotion recognition purposes is considered high-risk (Annex III – Point 6 (b))

[11] Pag. 48: Barrett, L. F., Adolphs, R., Marsella, S., Martinez, A. M., & Pollak, S. D. (2019). Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements. *Psychological Science in the Public Interest*, *20*(1), 1–68. https://doi.org/10.1177/1529100619832930.

[12] This is also the position of the EDPB and the EDPS, who are calling for the prohibition of AI used to infer emotions, except for very specified purposes (e.g. in the health sector, there could be applications where patient emotion recognition detection can be important);

will be excluded from the scope. This is for example the case of online profiling and personalisation techniques, content recommender systems that select what people see in their social media feeds. Also, a significant number of connected devices embedded with AI (e.g. smart meters, connected toys, virtual assistants) are not classified as high-risk AI.[13]

The risks created and potential for harm stemming from the myriad of AI systems that are and will increasingly be present in consumers' lives are not properly addressed by the regulation. Even if there is a basic requirement of transparency in Article 52, the scope of this provision is limited to certain AI systems and transparency alone is not sufficient.

Secondly, the 'high-risk' category is too narrowly defined as well.[14] The risks taken into consideration are limited to those of health and safety and the protection of fundamental rights[15], leaving out basic consumer rights, societal effects, impact on democracy, rule of law or environmental impact, as well as the potential for economic harm. For example, AI used to assess the eligibility of someone for a health or car insurance, or the cost of such insurance, would not be considered as 'high-risk' AI.

The Commission has competence to update the list of high-risk AI falling under Annex III. However, several strict conditions need to be fulfilled, making it very difficult to make use of such possibility in practice.[16] For example, it limits the possibility of expanding the scope to the areas already listed in Annex III.

BEUC in contrast supports a 'risk-based approach' where all AI (and not only high-risk) are subject to a minimum set of rules (starting with basic principles of transparency, fairness, accountability, non-discrimination, security, etc.). Then, the higher the risk, the stricter the specific requirements should become. A broader, more inclusive approach is necessary in the proposed Regulation.

3. For high risk AI applications, a conformity assessment by third parties should be the rule, not the exception

The proposal provides for far too much reliance on industry self-assessing that it complies with the rules.[17] This approach is not adequate as it does not take in consideration the complexity of the risks posed by AI and is likely not to be effective to protect consumers.

First, there is an evident conflict of interest: the entity assessing whether a certain product is in compliance with the rules is the same company who has an interest in placing the AI on the EU market as quickly as possible.

Second, a survey[18] about independent third-party testing shows that the compliance and safety of independently-checked products can be considerably higher than for products that rely simply on manufacturer's self-declaration of conformity.

[13] According to Article 44 (3) of the proposal, the manufacturer of these devices may need to apply AI standards under certain conditions.

[14] See Article 6 of the proposal;

[15] See Article 7 (1) b) of the proposal;

[16] See Article 7 of the proposal;

[17] See Article 43 of the proposal;

[18] http://www.ifia-federation.org/content/wp-content/uploads/2016/11/Consumer-Products-Safety-Study-2016.pdf

Therefore, a conformity assessment by independent third parties should become the rule, not the exception.

4. AI rights for consumers need to be added.

Overall, the consumer perspective is lacking in the proposed AI Act. Remarkably, 'user' in the proposal is only defined as 'business user'.[19]

More importantly, the proposal does not include any specific citizen or consumer rights – such as a right to transparency, right to explanation, the right to contest an algorithmic decision and obtain human oversight, or the right to submit a complaint in the case of a suspected infringement.

When it comes to transparency, except for high-risk AI[20], the proposal only envisages transparency obligations in very limited circumstances. In short, users need to be informed when dealing with AI such as chatbots, deepfakes or emotion recognition technology.[21]

Consumers should have a strong set of rights, given the risks that AI technology brings for them. Existing legislation, such as the GDPR, does not provide sufficient protection in an AI context.

Key rights such as the right to obtain an explanation of how a decision based on AI affecting them has been taken are not included in the proposed legislation but need to be added. Consumers should not depend on the processing of personal data as this is the case under EU data protection rules.[22]-[23]

5. Effective redress mechanisms for consumers are needed.

The proposal does not envisage any redress possibilities for consumers. As mentioned in the previous point, there is not even a right to complain before a supervisory authority nor an obligation for companies to provide for a complaint mechanism. For example, if a consumer is harmed by non-compliant high-risk AI or by the use of AI prohibited under Art. 5[24], the proposed rules do not foresee any rights or mechanisms for consumers to obtain redress. In consequence, the entity which is the most vulnerable to harms caused by AI is also the least protected. The AI Act must envisage a structure that would furnish individuals with horizontal rights to seek remedies (e.g., compensation for damages) and to protect them. This should also include a reversal of the burden of proof for all AI interacting with or affecting individuals. Reversal of the burden of argumentation/proof establishes that it would be for the supplier of an AI to demonstrate that it complies with the law.[25]

[19] See Art. 3 (4) of the proposal;
[20] See Art. 13 of the proposal;
[21] See Article 52 of the proposal;
[22] Article 22 of the GDPR sets out that the data subject has the right not to be subject to automated decision-making. However, this right is restricted to fully automated processing of data and does not apply in a number of cases, such as when the decision making is based on users' consent or if there is not a legal or similar significant impact on the individual;
[23] Opinion of the German Data Ethics Commission, Executive summary, § 44, p. 21;
[24] See Chapter 1 above;
[25] https://www.beuc.eu/publications/beuc-x-2021-018_eu_consumer_protection.0_0.pdf, at 75

Furthermore, the proposal does not include the possibility of harmed consumers to be represented by an NGO, including consumer organisations, in the exercise of their rights. An article similar to Art 80 GDPR (Representation of data subjects) or Article 68 of the proposal for a Digital Services Act (Representation) should be introduced. In the context of the AI Act, this representation shall not be subject to a mandate.

Also, to enable collective redress actions, this proposal should be included in the Annex of the Representative Actions Directive[26]. A similar provision was included in the Commission's proposal for a Digital Services Act.[27]

6. The governance and enforcement structure must be clear and ensure an effective and consistent application of the rules at European and national level

The proposed governance and enforcement structure mainly rests at national level and raises issues in relation to the obligations, competences and powers of the different actors involved[28] and the different processes envisaged.

For example:

- The need to ensure a coherent and coordinated EU-wide enforcement. While the Commission plays a central role if a national supervisory authority notifies its intention to adopt measures against an AI system in its territory[29], the Commission has no powers to proactively take the lead in case of inaction by national authorities. The autonomy and powers of the European AI Board[30], comprised of high-level representatives of the national supervisory authorities and chaired by the Commission, also seem quite limited.

- There is a need to clarify potential overlaps with existing bodies such as the European Data Protection Board, as well as the role of Data Protection Authorities – a view that other stakeholders also share[31].

- It is also important to ensure a common approach when it comes to the cooperation between the different competent authorities and supervisory authorities at national level, to ensure effective and swift enforcement as well as to avoid different approaches by Member States.

- Given the lack of redress mechanisms for consumers in the proposal, there is no authority that is entrusted with dealing with consumer complaints in case of breaches of the regulation.

[26] Directive (EU) 2020/1828 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC;
[27] See Article 72 of the Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC;
[28] Namely: the European Artificial Intelligence Board (EAIB), the national competent authorities, the national supervisory authority, the Commission, the European Data Protection Supervisor (EDPS) and the AI system providers);
[29] See Articles 65 (5) and 66 of the proposal;
[30] See Articles 56 – 58 of the proposal;
[31] See, for example, Access Now: https://www.accessnow.org/eu-minimal-steps-to-regulate-harmful-ai-systems/.

- Providers of high risk AI systems are only obliged to report serious incidents or malfunctioning which constitute a breach of Union law intended to protect fundamental rights. This leaves out breaches of fundamental rights stemming from non-high risk AI systems, as well as any serious incidents or malfunctioning which are not directly related to fundamental rights. For example, a faulty AI used in an energy distribution grid can have a serious impact on the finances and wellbeing of consumers by inadvertently cutting off their energy supply or overcharging them. This would not be covered under the proposal.

It is key to have a clear and coherent oversight and enforcement structure to guarantee an effective and consistent protection of consumers all across the EU.