Raising standards for consumers

POSITION PAPER

ANEC comments on the European Commission proposal for an Artificial Intelligence Act

(Regulation laying down harmonised rules on artificial intelligence and amending certain Union legislative acts)

COM(2021) 206 final, 2021/0106 (COD)

Contact: Chiara Giovannini

Chiara.Giovannini@anec.eu

ANEC is supported financially by the European Union & EFTA

Ref: ANEC-DIGITAL-2021-G-071 July 2021

European Association for the Co-ordination of Consumers Representation in Standardisation aisbl

Rue d'Arlon 80 - B-1040 Brussels, Belgium
T: +32-2-7432470 / anec@anec.eu / www.anec.eu

1 | Executive Summary

ANEC welcomes the European Commission consultation on the proposal for a Regulation laying down harmonised rules on artificial intelligence and amending certain Union legislative acts and we are pleased to share our views on the future European legislation on AI.

As a member of the Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission and of the CEN-CENELEC Focus Group on Artificial Intelligence and CEN-CLC Joint Technical Committee 21 on AI, we focus our replies on the use of standards and related legal provisions to shape the European approach for Trustworthy AI.

In reply to the European Commission Inception Impact Assessment from 2020 on a proposal for a legal act of the European Parliament and the Council laying down requirements for Artificial Intelligence, ANEC expressed support for a legislative instrument establishing mandatory requirements for all applications. The new rules should cover risks posed by AI systems in a proportionate manner, with more stringent rules for high-risk applications [1].

We refer to the BEUC's position for other aspects of consumer relevance, such as the biometrics techniques and their impact on consumers, the list of high-risk AI application of Annex III and the specific AI consumer rights, including redress[2].

2 | Scope and definitions

While we agree that there are standalone AI software applications (chatbots, facial recognition etc…), we also think that there are many AI applications where it is the combination with hardware or other connected device that is fundamental to the risk. For example, certain AI facial recognition software has to be connected to a camera in order to work. If it is a simple low-resolution camera, the system capability is limited and so is the risk. If the AI software is connected to a high-performance camera, a night vision camera or through a network of many cameras, the risk is very significant. By treating the 'AI system' as software alone and ignoring the hardware, the understanding and controlling of the possible risk is limited.

We therefore suggest that a new definition is added for AI systems:

'*Artificial intelligence system' (AI system)* means a combination of AI with hardware or other devices that for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, *movements, actions* or decisions influencing the environments they interact with.'

[1] https://www.anec.eu/images/Publications/position-papers/Digital/ANEC-DIGITAL-2020-G-106-.pdf
[2] We also believe that new consumers rights should be enshrined, for all AI systems, and not only high-risk applications, as follows: Right to Transparency, Explanation, and Objection, Right to Accountability and Control, Right to Fairness, Right to Safety and Security, Right to Access to Justice, Right to Reliability and Robustness.

From the point of view of consumers, the concept of "intended use" does not correspond with real-life situations and neglects the expectations of consumers in modern society. In order to cover the consumer behaviours and what influences them, we suggest introducing the concept of **foreseeable use** (and not only misuse), based on the following elements: the technical and functional characteristics of the AI system, the factual and human behaviours and physical characteristics, the relation with other products and the use with other products. If use is reasonably foreseeable, then the product should not cause harm regardless of whether the use is as intended or not. We think that the presentation of the product is also an important element to take into account because it influences the consumer behaviour.

We welcome the reference to the concept of **substantial modifications**. However, we think that it should also cover the modifications to the foreseeable use and not only intended purpose for which the AI system has been assessed.

3 | Prohibited AI

We welcome the strong stance against certain AI practices which is in line with the European approach to Trustworthy AI. However, we think that there are several loopholes and exceptions which leave the door open for discussion and interpretation.

We fully support the EDPS/EDPB call for the ban on the use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination such as social scoring[3]. We ask for the proposed AI regulation to ban these dangerous AI practices.

Stronger rules are needed to determine how and by whom **biometrics** technology can be used and the guarantees for citizens and consumers. Considering the high risk of abuse, discrimination and violation of fundamental rights to privacy and data protection, the European Union must develop a strong, privacy-protective approach for biometrics systems before they are largely used in public spaces by private operators and not only public enforcement authorities (as currently done in the proposed AI Act).

'Personally identifiable biometric indicators' could be identified. They would cover a range of AI practices including behavioural biometrics like walking patterns or touch screen usage, allowing for a clear assessment of the risk for consumers and possible prohibition to protect consumers.

About the protection of groups of persons with **vulnerabilities**, we would like to remind that everyone can be in vulnerable situation at a given point in time. This is the case when consumers are exposed to "black box" technology and other AI practices.

We also refer to our comments about the concept of foreseeable use (and not only misuse or intended use) in the context of the intentional effects of the AI to be prohibited, which we think is too restrictive in terms of dangerous AI practices.

[3] https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-call-ban-use-ai-automated-recognition_en

4 | High risk AI systems

4.1 Classification rules for high-risk AI systems (art. 6)

The reference to the conformity assessment regimes contained in the existing product legislation/Union harmonisation legislation has the consequence that the majority of AI consumer products such as toys or connected appliances would undergo only the manufacturer self-assessment, even if posing a high-risk to consumers. This is because existing product legislation uses **conformity assessment modules** that were developed for the type of risks addressed by such sectoral legislation (eg: chemical, mechanical, etc) and therefore do not include risks posed by AI.

As the European Commission's assessment of product safety and liability legislation showed, there are gaps in present legislation and new AI related aspects such as explicability require new legal provisions, especially for enforcement purposes. The AI Act should be based on and explicitly refer to the precautionary principle.

We think that new specific rules should be adopted in the draft AI Regulation, to make the appropriate risk assessment of all AI products, taking into account the nature of the hazard and the likelihood of its occurrence. Based on the assessment results, different rules can be applied in a proportionate manner.

Any AI system has the potential to cause harm so identifying a limited group as high-risk and ignoring the rest can result in dangerous systems slipping through.

In order to assess whether the AI system is posing a high or low risk, criteria such as likelihood of the harm occurring, immediacy of the harm, the foreseeable use of the AI system (and not only the intended use which is not covering the potential effects of machine learning) have to be taken into account too. In addition, provisions have to deal with how uncertainties and assumptions impact the risk assessment. In addition to cyber risks, personal security risks, risks related to the loss of connectivity and mental health risks, the risks to the environment should not be forgotten.

We believe that product liability rules should be updated to ensure consumers are protected when they face problems with their digital goods.

Annex II with the list of List of Union harmonisation legislation based on the New Legislative Framework should also refer to the Low Voltage Directive (2014/35/EU) as many AI consumer products will be domestic robots or autonomous domotic environments.

4.2 Requirements for high-risk AI systems (Chapter 2)

We welcome the use of most of the requirements of the HLG Ethics Guidelines for Trustworthy AI into specific requirements for 'high-risk' AI. However, we regret that the requirement about **'inclusivity, non-discrimination and fairness'** is not expressly present in the draft act. We believe that it should be made mandatory, especially in the context of data and data governance and design or purpose-setting.

In terms of accountability, another important Ethics Guidelines requirement, we think that new provisions should be introduced about **complaint and redress-by-design**

mechanisms to allow users and consumers to report problems with the AI system and obtain a solution.

We also reiterate our comments about the consideration of the foreseeable use and not only the intended purpose of the AI system when ensuring compliance with the requirements.

Standards can be used to embed security requirements at the design phase of the product and to ensure compliance with legal requirements. However, for a standard to be effective, its provisions need to be clear, unambiguous and replicable. This is particularly important in the case of AI systems: because security breaches can take multiple forms, objective and measurable requirements are needed to allow for the objective assessment of the conformity level of AI systems. This might prove to be particularly challenging for Harmonised Standards covering the AI systems in Annex III.

We expect European standards to specifically address European values and fundamental rights and not just adopt International Standards which might not reflect our values and principles. Standards can be a tool to introduce values/principles in product/service design (eg: privacy by design) as they can embed principles in technologies, underpinning legislation. As consumers, we want to be sure that consumer protection principles will be reflected by design in the future European standards on AI.

But it is not only about the 'what is standardised', it also about the 'how standards are made'.

While the identification of strategic priorities in the standardisation development of digital technologies by the European Standardisation Organisations (ESOs) is key to ensure European values and principles are preserved and protected, a reflection has to take place about the decision-making processes inside the ESOs. This is not only about the governance but mainly about technical decisions and comments.

And because the European values and principles include consumer protection, we are concerned by such developments. Openness, inclusiveness, global markets and international trade should not preclude the protection of European values and principles.

We also call for increased **inclusiveness of the standardisation process** in order for consumers of all ages and abilities to be able to effectively participate in the development of the standards. Unfortunately, sometimes it is not the case. This does not bode well for the future development of the standards, which should be based on the consensus of all the concerned stakeholders.

4.3 Implementing acts establishing common specifications (art. 41)

The European legislators delegate to the European Commission the power to request the European Standardisation Organisations (ESOs) to develop standards in line with the principles of Regulation 1025/2012 (consensus, coherence, transparency, openness, independence of special interests, efficiency). However, as the ESOs can refuse to accept a standardisation request, which validity ceases if not accepted, it is opportune to foresee a fall-back solution in case of lack of Harmonised Standards.

However, we suggest that the Commission is invited to conduct extensive **stakeholders' consultations** on the draft implementing acts containing the technical

specifications, beyond the usual comitology procedures, in order to ensure that the views of all stakeholders are duly considered.

4.4 Presumption of conformity with certain requirements (art 42)

We think that the provision about presumption of conformity with certain requirements (art 42.1) represents an important loophole which should not be allowed. Despite the reference to the intended purpose only, we doubt the existence of such closed and constrained AI systems able to ensure a total control on the data they use.

We wonder whether the reference to future **cybersecurity** scheme adopted to meet the cybersecurity requirements set out in Article 15 is appropriate, bearing in mind the uncertainty about the existence of such future schemes and the different scope of the two Regulations.

4.4 Conformity assessment (art. 43)

We reiterate our comments about the reference to the conformity assessment regimes contained in the existing product legislation/Union harmonisation legislation, which is not enough to protect consumers as existing product legislations are based on the risks addressed by such legislation (eg: mechanical, electrical, etc), and not the risks posed by AI.

We think that new specific rules should be adopted in the draft AI Regulation, to make the **appropriate risk assessment of all AI products**, taking into account the nature of the hazard and the likelihood of its occurrence. Based on the assessment results, different conformity assessment modules can be applied, in a proportionate manner.

About the machine-learning of high-risk AI systems which would not require a new conformity assessment as not resulting in substantial modifications (art.43.4), we doubt the existence of such closed and constrained/pre-determined AI systems able to ensure a total control on the data they use.

4.5 CE marking (art. 49)

Even though **CE Marking** is not intended as a mark for consumers, its appearance on many products (or their packaging) is widely recognised by consumers and therefore can be interpreted by them as a consumer mark and misled them. ANEC wants to see CE Marking relegated to the technical file of a product that European law also requires.

After over twenty years of the Internal Market for products, CE Marking should no longer be allowed to mislead and confuse European consumers, not only for products falling under the AI regulation, but for all consumer products that require CE marking[4].

5 | Transparency obligations for certain AI systems

ANEC believes that having sufficient and adequate knowledge about the safety and other aspects of the products consumers buy and use, is an essential consumer need. Information should be reliable, understandable and transparent. Warnings should only

[4] https://www.anec.eu/publications/position-papers/201-anec-position-paper-on-ce-marking-caveat-emptor-buyer-beware

be complementary to strict safety measures and should not exonerate manufacturers from ensuring that products do not present a risk to consumers.

However, the inherent **information asymmetry** associated with AI or an evolving/machine learning system, makes the function of information different from information linked to traditional, non-AI products (e.g. Ecolabel) where the technological content of the product is "static". The information is not very helpful if the behaviour of products changes over time but the information stays the same. One reason more for us to seriously wonder about the inclusion of emotion recognition system or a biometric categorisation system and 'deep fake' in the level of low-risk AI systems, especially as consumers will not benefit from the right to opt-out of the system.

6 | Information sharing and market surveillance

Market surveillance authorities should have sufficient resources to enforce the AI requirements. We stress the need to ensure national supervisory authorities have the **financial, technical and technological means** to carry out their mission. The possibility of imposing mandatory inspection fees – as done in Food Safety legislation- should be explored. The proceedings of the fines should be used to finance the market surveillance activities.

6.1 Reporting of serious incidents and of malfunctioning (art.62)

We think that serious incident or any malfunctioning of AI having an impact on consumer safety should also be reported. We refer to our long-lasting call for a **pan European accidents and injuries database** in order to assess whether a product is posing a high risk for consumers, with the aim of achieving a high quality, representative and up-to-date data sample for the entire Single Market[5].

6.2 Procedure for dealing with AI systems presenting a risk at national level (art.65)

The **precautionary principle** allows market surveillance authorities to take temporary and preventive measures in the absence of a definitive proof of harm to consumers or the environment. As such, we think that this fundamental principle should be present in the AI Act which is dealing with new technologies and unforeseen effects.

In current market surveillance practice, legal obstacles prevent an exchange of information in both the harmonised and non-harmonised areas about dangerous products with other countries/jurisdictions. It is therefore important that the AI Act provides for a strengthening of **international cooperation** by allowing the exchange of information beyond confidentiality rules.

ENDS

[5] European consumer safety needs solid injury data, ANEC-EuroSafe position paper, November 2020

ANEC is the European consumer voice in standardisation, defending consumer interests in the processes of technical standardisation and the use of standards, as well as related legislation and public policies.

ANEC was established in 1995 as an international non-profit association under Belgian law and is open to the representation of national consumer organisations in 34 countries.

ANEC is funded by the European Union and EFTA, with national consumer organisations contributing in kind. Its Secretariat is based in Brussels.

Designed by AdGrafics.eu

ANEC

Raising standards for consumers

European association for the coordination of consumer representation in standardisation aisbl

Rue d'Arlon 80
B-1040 Brussels, Belgium

+32 2 743 24 70

anec@anec.eu

www.anec.eu

EC Register of Interest Representatives:
Identification number 507800799-30
BCE 0457.696.181

@anectweet

ANEC is supported financially by the European Union & EFTA