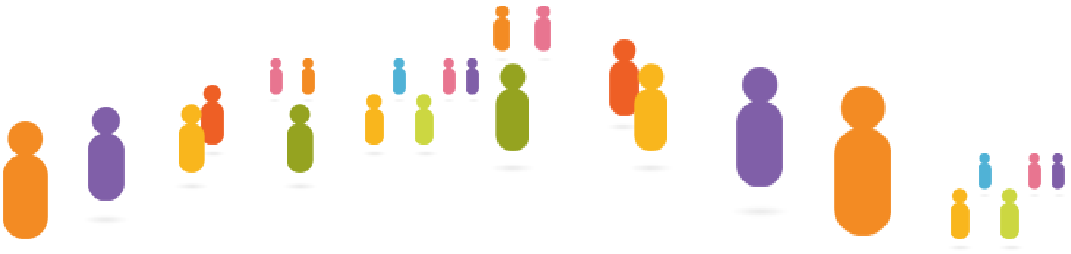
BEUC The European Consumer Organisation

The Consumer Voice in Europe

REGULATING AI TO PROTECT THE CONSUMER

Position Paper on the AI Act



Contact: **Frederico Oliveira da Silva and Kasper Drazewski**

digital@beuc.eu

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2021-088 - 07/10/2021

Why it matters to consumers

AI products and services, such as virtual assistants and facial recognition tools, are already changing consumer markets and our societies. It is a technology which carries huge expectations of improving and making consumers' lives more convenient. But the use of AI also comes with great risks and has major implications for consumers' autonomy and self-determination, their privacy, their capacity to interact with products and services and, ultimately, in the ability to hold businesses responsible if something goes wrong. The AI Act must provide consumers with the rights and protections they need to be at ease when using AI, while also allowing space for innovation and, more broadly, ensuring EU's fundamental rights and values are respected.

Summary

Regulating AI is crucial to ensure a high level of consumer protection and a fair, safe and sustainable development of our society. BEUC welcomes that the Commission has taken the initiative in this regard. However, the AI Act proposal requires substantial improvements to guarantee consumers have the protections they need and can trust AI to respect their rights and freedoms.

This position paper contains a series of recommendations for the Commission's AI Act proposal (scope, definitions, harmonisation, prohibited practices, risk and conformity assessments and other obligations for AI systems, standardisation, enforcement, etc).

Key BEUC recommendations:

The proposal must have a broader scope and impose basic principles and obligations, e.g. on fairness, accountability and transparency, that apply to all AI systems.

- The scope of the AI Act should be broadened to adequately regulate AI systems other than those it currently classifies as 'high-risk', such as smart meters, AI-powered connected toys, virtual assistants or AI that organises what people see on social media.

- All AI systems employed in the EU, including medium- and low-risk systems, should respect a set of common principles established in the AI Act (e.g. transparency, fairness, non-discrimination).

- The existing list of 'high-risk' applications in Annex III should be expanded to include additional AI applications. For example, AI used to assess insurance premiums and AI payment and debit collection services.

The list of forbidden AI practices in Article 5 must be extended and strengthened to include harmful practices which are currently not covered.

- Articles 5 (1) a) and b) should include AI practices that manipulate someone in a way that can cause them economic harm.

- Articles 5 (1) a) and b) should cover AI practices where its 'intended purpose' or 'reasonably foreseeable misuse' can manipulate someone and lead to physical, psychological or economic harm.

- Art. 5 (1) b) should also apply to AI used to exploit vulnerabilities other than those related to children or of physically- or mentally-disabled people. For example, it should protect consumers made vulnerable through the use of persuasion profiles and personalisation practices (digital asymmetry) or through temporary vulnerabilities (e.g. grief, sorrow, emotional distress) who are not associated to group of people due to their age, physical or mental disability.

- A broad reversal of the burden of proof putting the onus of demonstrating compliance on the entity using the AI system in all disputes involving individuals must be introduced to reinforce the prohibitions of Article 5.

- Regarding social scoring, Article 5 (1) c) should introduce a general ban on AI used by both public and private bodies to evaluate the trustworthiness of an individual based on their social behaviour or other personal attributes, such as someone's preferences, emotions, health or intelligence.

- The use of remote biometric identification systems by private entities in public spaces should be banned, without exceptions.

- Article 5 of the AI Act should ban the use of emotion recognition AI except in very specific circumstances related to health or research purposes, in line with the recommendations of the EDPB and EDPS.

- The AI Act should prohibit the use of AI for which the scientific validity is unproven or the claimed benefits have been debunked by science.

Consumers must have a strong set of rights and access to effective remedies and redress mechanisms in case of harm, including collective redress.

- Consumers should have the right to be given a clear explanation about how an AI system affecting them works, and the right to object to an algorithmic decision that has a significant impact on them.

- The proposal must also grant consumers the means to seek justice and redress in case of harm. The AI Act must include:

    - A right for consumers to complain to a national authority or launch a legal action in court when an AI system or practice which affects them infringes the Regulation. This should include a right to receive compensation for material or non-material damages suffered.

    - An obligation for companies to make a complaint mechanism available to consumers. Companies must be obliged to react to those complaints within a short period of time.

    - An article allowing consumer organisations, or more broadly civil society organisations, to represent individual consumers in the exercise of their rights under this Regulation. They should also be allowed to act in the 'general interest' (i.e. be able to bring forward complaints without a mandate from an individual, when they consider that an AI system or practice is infringing the rules).

- A provision that adds the AI Act to the Annex of the Representative Action Directive (RAD), which lists the laws where it is possible to file a representative action. It must be possible to file collective redress or injunctive actions in case of non-compliant AI.

The conformity assessment procedure applicable to 'high-risk AI systems' (Article 43) must be strengthened.

- Third party assessment should be the rule to assess the conformity of 'high-risk AI systems'. Self-assessment should only be allowed when AI systems are not considered to be high-risk.

- For high-risk AI systems, the results of the conformity assessment procedure and all relevant documentation must be notified to the relevant market surveillance authority before the product is placed on the market and made available to the public.

Harmonised standards should only be used to define technical requirements, not to define or apply legal principles and fundamental rights.

- Harmonised standards must not be used to define or apply fundamental rights, legal or ethical principles. Their use should be limited to implement technical aspects. In this regard, a standard should, for example, not be used to determine what types of biases are prohibited under Art. 10 (2) f).

The governance structure and the enforcement mechanisms of the AI Act by national authorities needs to be clarified and improved.

- Enforcement should be reinforced on a technical level with the creation of a highly specialised body of technical experts designated by the Commission. Such a body should assist national authorities and the Commission in the technical aspects of their investigations, and have the competence to issue non-binding opinions about specific cases brought up by the national authorities.

- To ensure a coherent and consistent application of the AI Act, it is important to specify in Article 65 (2) that those authorities which start an investigation into a suspicious AI system must inform their counterparts in the other Member States within the AI Board.

- The procedure foreseen for solving disagreements between national authorities in Article 66 should not be limited to actions started by Member States' authorities. The European Commission should be able to start an evaluation procedure about an AI system under this provision whenever (i) it has sufficient reasons to believe that that an AI system presents a risk, (ii) no market surveillance authority started an investigation under Article 65 (2) and (iii) the AI system affects consumers in more than one Member State.

Contents

1. Introduction

On 21st April 2021, the European Commission published the proposal for a Regulation laying down harmonised rules on Artificial Intelligence and amending certain Union legislative acts ('Artificial Intelligence Act').[1]

Artificial intelligence (AI) has the potential to bring many benefits for consumers. It can power new products and services and help make daily life easier and less burdensome (via e.g. personalised services, augmented reality applications, AI-powered healthcare tools that can help detect diseases quicker, and automated vehicles). However, AI also comes with significant risks and challenges for consumers. For example, the use of AI to maximise user monetisation can lead to increased risks of algorithmic 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.

64% of respondents in Belgium, Italy, Spain and Portugal and 52% of respondents from Denmark, France, Germany, Poland and Sweden 'agree' or 'strongly agree' that companies use AI to **manipulate consumer decisions and abuse personal data**

BEUC AI survey 2020

Consumers are concerned with the rollout of this technology. BEUC member organisations conducted an EU-wide survey to see what consumers think about AI.[2] A large majority of respondents perceive AI to be somewhat or even very useful to them in different areas, especially when it is used to predict traffic accidents (91%), their health (87%) or financial problems (81%). However, respondents have highlighted the risks associated to this technology. In Belgium, Italy, Portugal and Spain, most respondents (64%) agree or strongly agree that companies are using AI to manipulate consumer decisions.

Also, there is a significant lack of trust: when asked about their level of trust in that their privacy is protected when using AI devices, a large majority of consumers state this to be medium or low. An average 50% of Belgian, Italian, Portuguese and Spanish as well as 45% of Danish, French, German, Polish and Swedish respondents have low trust in the protection of their privacy with wearables.

Current EU rules are insufficient to ensure a high level of consumer protection when it comes to AI. For instance, the consumer's right to be informed about the use of AI and to contest automated decisions is very limited in scope and only apply in certain situations. Also, existing EU laws do not guarantee that AI systems need to be safe.

From this perspective, BEUC welcomes that the European Commission has put forward a much-needed legal instrument aimed at regulating AI.

Although the AI Act proposal marks a welcome and necessary step, regretfully, it generally fails to address consumers' core concerns and expectations. This is particularly due to its narrow scope, focused on a pre-defined list of so-called 'high risk AI'

[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.

[2] https://www.beuc.eu/publications/survey-consumers-see-potential-artificial-intelligence-raise-serious-concerns/html

applications, and the general disregard of the particular dangers posed by AI systems to consumers' rights. Moreover, the proposal relies heavily on industry's own unvetted assessment of compliance with legislation and fails to put forward a robust governance and public/private enforcement system. Finally, the methodology of listing specific AI systems that the proposed regulation would apply to seems ill-adapted to all future applications of AI that have not yet been developed.

In this paper, we address these shortcomings and suggest improvements to ensure that the legislative proposal provides the rights and protections that consumers need, while also giving space to innovation and respecting our fundamental rights and values.

2. Objectives and consumer protection gap

The proposal aims to lay down a uniform legal framework for the development, marketing and use of artificial intelligence in conformity with the European Union's values, such as a high level of protection of health, safety and fundamental rights.[3] The latter are to be understood as consistent with the Charter of Fundamental Rights of the European Union[4] and include human dignity, respect for private and family life, protection of personal data, freedom of expression and information, non-discrimination, or a right to an effective remedy and to a fair trial,[5] as well as the duty to ensure a high level of consumer protection as enshrined in Article 38 of the Charter.

However, beyond the declarative non-binding layer in the recitals, consumer protection is lacking in the proposed AI Act. The proposal does not refer to protection of consumers from the adverse impact of AI among the legislative objectives of the AI Act. Consumers are not granted horizontal rights under the proposal and are excluded from the conceptual framework as definition of 'user' in the proposal is only defined as an institutional or business user.[6]

BEUC recommendation:

- Ensuring a high level of protection for public interests, such as health and safety in general, the protection of consumers, the protection of the environment and of fundamental rights I risks and potential harms caused by artificial intelligence should be explicitly mentioned as legislative objectives of the AI Act in Article 1.

3. The implications and risks of maximum harmonisation

An important aspect in understanding the role and implications of the AI Act is that of the intended level of harmonisation and the very broad material scope covering all AI systems that fall under its definition in Article 3 (1). A maximum harmonisation instrument leaves no ability for Member States to regulate further and prevents any more restrictive and thus protective regulation within that area on a national level.

This is addressed explicitly in the proposal. The proposal states it prevents "Member States from imposing restrictions on the *development, marketing and use of AI systems*, unless explicitly authorised by this Regulation"[7] (emphasis added). Coupled with the broad

[3] Recital 1 of the proposal.

[4] Recital 13 of the proposal.

[5] Recital 28 of the proposal, referencing the Charter of Fundamental Rights of the European Union.

[6] Article 3(4) of the proposal.

[7] Recital 1 of the proposal.

definition of AI systems included in the text,[8] this would leave no room for any further legislation in Member States concerning AI, despite the scope of the proposal covering only high-risk systems. [9] This would mean that the proposal would:

- establish regulatory requirements for a narrow group of AI systems defined by the proposal as high-risk, while

- precluding Member States from establishing further restrictions on a broad array of AI systems without imposing any of its own.

BEUC recommendations:

- Introducing maximum harmonisation rules for all AI systems via the AI Act in its current form cannot be deemed fit for purpose due to its substantive scope being focused almost exclusively on a narrow list of systems which it labels as high-risk.[10]

- Recital 1 should be amended to clarify that Member States can establish additional limitations than those established in the AI Act provided that they are justified on grounds of public interest and the protection of individuals.

4. Main definitions and concepts (Article 3)

4.1. AI system

Many different definitions of AI and AI systems are in circulation. The Commission's 2020 White Paper on AI speaks broadly of "*technologies that combine data, algorithms and computing power*",[11] while its 2018 Communication[12] defined AI as "*systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals*". The Commission's High Level Expert Group[13] (HLEG) published its own extensive definition of AI systems in 2019, which now echoes in the approach taken in the AI Act proposal.[14]

While refraining from defining 'artificial intelligence' (AI) as such, Article 3 (1) of the proposal defines an 'AI system' as one able to, for a given set of human-defined objectives,

[8] See Section 4.1 below.

[9] Michael Veale, Frederik Zuiderveen Borgesius, Demystifying the Draft EU Artificial Intelligence Act (forthcoming in (2021) 22(4) Computer Law Review International) at 21.

[10] See also the comments in Section 6.1.3 on systems other than high risk.

[11] https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf, p. 2.

[12] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, Brussels, 25.4.2018 COM(2018) 237 final.

[13] Of which BEUC was a member.

[14] HLEG proposed to define AI systems as "software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems." Independent High-Level Expert Group on Artificial Intelligence, A definition of AI: main capabilities and disciplines, 2019

generate outputs such as content, predictions, recommendations, or decisions influencing the environments it interacts with, using techniques and approaches defined in Annex I as machine learning approaches, logic- and knowledge-based approaches or statistical approaches.[15]

This definition is broad and tied to the possible uses of technologies and approaches listed in Annex I while only offering suggestions of outputs such systems may produce. In doing so, it avoids the pitfalls of layman definitions linking the operation of AI to that of human intelligence and thus significantly narrowing down their scope.

Since the AI Act aims to lay down a uniform legal framework for (all) AI, it is important to ensure that it does not shy away from establishing ground rules for all AI systems. To this end, the definition of AI systems must be both broad and able to cover applications to be developed in the future, and not be prone to misinterpretation so that simple tools like Excel spreadsheets using statistical formulas don't get included.

BEUC recommendations:

- To address the numerous definitions in circulation, the proposal should clarify in Recital 2 that its references to 'AI systems' also apply to AI as such, as per the HLEG AI definition paper.[16]

- To avoid any misunderstandings, Recital 6 should clarify the reach of the definition of 'AI system' and give some examples of tools and systems, such as spreadsheets with statistical formulas, that would typically not fall under the definition of 'AI system'. In this regard, Annex I should not be amended.

4.2. User

As mentioned above, the definition of 'user' in Article 3(4) of the proposal refers to "any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity".

This approach excludes individuals using AI systems as 'users' under the AI Act unless they are doing so in their professional capacity, as well as those individuals who are subject to the use of an AI system.[17]

BEUC recommendation:

- To ensure a high level of consumer protection, the AI Act must introduce a definition of 'consumer'.

4.3. Risk

The proposal presents a 'risk-based' approach relying on an *ex ante* classification of AI systems, with the high-risk category being the main subject of regulation (see section 5 for a discussion on the classification and its implications).

[15] Annex I (a)-(c).

[16] See fn. 14 above.

[17] Ada Health GmbH: Ada Website, URL: https://ada.com/app/

While the proposal does not define 'risk' as such, it offers numerous hints to this effect. A 'risk of harm to the health and safety, or a risk of adverse impact on fundamental rights' is offered as a criterion for updating the list of high-risk AI systems in Annex III.[18]

Moreover, Article 65 (1) defines an AI system presenting a risk as a "*product presenting a risk*" definition under Article 3 (19) of Regulation 2019/1020[19] but only "*insofar as risks to the health or safety or to the protection of fundamental rights of persons are concerned*",[20] thus leaving out all other risks contemplated in that Article.[21]

With the exception of a high level of environmental protection, which is included in this assessment under Recital 28, other risks posed by AI to individuals and society (e.g. risks to democracy or rule of law), despite all being highlighted by the HLEG Ethics Guidelines for Trustworthy AI,[22] are thus left outside of the scope of this Regulation.

Risks to societies, such as attention-maximising personalisation algorithms in recommender systems, are not included. Similarly, other risks which are highly pertinent to consumers in the digital sphere, i.e. risks of adverse impact on consumers' agency, autonomy of choice, access to goods and services, unfair discrimination and economic harm, are also not addressed by the proposal.

BEUC recommendation:

- Risks of AI having an adverse impact on consumers' agency, autonomy of choice, access to goods and services, unfair discrimination and economic harm, privacy and data protection, as well as societal risks should also be explicitly addressed in the definition of an 'AI system presenting a risk' under Article 65 (1).

4.4. Harm

Similarly to risk, 'harm' is flagged in the Explanatory Memorandum as needing definition.[23] However, the term remains undefined in the proposal despite its frequent use. It is often used in reference to health and safety of persons and fundamental rights[24] but also in a general sense, in contexts such as public interests and rights[25] and regulatory sandboxes.[26]

A detailed guidance on harm (clarifying the types and ways in which AI can cause detriment) should be introduced to the recitals to help interpreting the existing references to individual harm. This is particularly the case of use of AI systems intended[27] for material

[18] Article 7(1) in conjunction with Article 73 and 84(1) of the proposal.

[19] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products ('Market Surveillance Regulation').

[20] Article 65(1): '*AI systems presenting a risk shall be understood as a product presenting a risk defined in Article 3, point 19 of Regulation (EU) 2019/1020 insofar as risks to the health or safety or to the protection of fundamental rights of persons are concerned*.'

[21] These are products having the potential to affect adversely health and safety of persons in general, health and safety in the workplace, protection of consumers, the environment, public security and other public interests, protected by the applicable Union harmonisation legislation, to a degree which goes beyond that considered reasonable and acceptable in relation to its intended purpose or under the normal or reasonably foreseeable conditions of use of the product concerned, including the duration of use and, where applicable, its putting into service, installation and maintenance requirements (following Art. 3(19), Market Surveillance Regulation).

[22] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419

[23] Id.

[24] See e.g. Recital 28, 32, Article 7(1)b and 7(2), Article 13(3)b of the proposal.

[25] Recital 4 of the proposal.

[26] Article 53(4) of the proposal.

[27] Recital 16 places these prohibitions in the context of AI systems 'certain AI systems intended to distort human behaviour' rendering them even more narrow than their wording would suggest.

distortion of a person's behaviour that is likely to lead to physical or psychological harm, covered under Article 5(1) (a) and (b). Applying a 'common sense' definition of harm in this context may lead to difficulty in applying these provisions in practice, particularly given the need to establish intended use[28] and the extremely narrow scope of these provisions.[29]

Harms which are collective rather than individual, as well as those which build up over time rather than being caused by a one-off event, are not covered. This is the case of recommender systems combined with hyper-personalisation, engagement and impact on children.[30] Harm resulting from users' interaction with an AI system is seemingly also ruled out by Recital 16 which precludes presumption of intent *"if the distortion of human behaviour results from factors external to the AI system which are outside of the control of the provider or the user*".

This raises the question to what degree harm caused by e.g. social networks or content recommender sites, can even be considered in this context. Lastly, downstream harms, where one agent deploys an AI for classification of individuals and another entity (e.g. a dating service) uses this classification in a harmful manner, are also difficult to address under this proposal.[31]

BEUC recommendations:

The recitals should include detailed guidance on the concept of harm, to clarify the following:

- a clear concept of how 'harm' is to be understood, e.g. by means of referencing the EU general risk assessment methodology[32] definition of 'harm' as injury or damage to the health of people or damage to property, economic harm to consumers, damage to environment, security and other aspects defined in the scope of New Approach directives, complemented by collective harms such as harm to society;

- the manner in which 'harm' is created, including:

    - by single events and through exposure over time to harmful algorithmic practices; as well as

    - through action distributed among a number of actors where the entity causing the harm is not necessarily that which uses the AI;

    - causation of harm through uses other than intended, to avoid narrowing down the framework to systems 'intended to distort behaviour' as Recital 16 suggests, and to avoid the pitfall of basing harm on the presumption of an intention which may

[28] A good example is general-purpose AI or AI as a service; see Cobbe, Jennifer and Singh, Jatinder, Artificial Intelligence as a Service: Legal Responsibilities, Liabilities, and Policy Challenges (April 12, 2021). Forthcoming in Computer Law & Security Review, Available at SSRN: https://ssrn.com/abstract=3824736 or http://dx.doi.org/10.2139/ssrn.3824736

[29] See more specifically Section 5 on the list of prohibited practices.

[30] Borgesius, Veale (2021) at 4.

[31] Id, at 5.

[32] EU general risk assessment methodology (Action 5 of Multi-Annual Action Plan for the surveillance of products in the EU (COM(2013)76), https://ec.europa.eu/docsroom/documents/17107/attachments/1/translations/en/renditions/native

not even exist or be hidden/impossible to prove (such as in case of AI as a service, or e.g. stalkerware sold as child trackers[33]).

4.5. Intended purpose and misuse

A prominent parameter in the proposed framework is the 'intended purpose' of an AI system, which is defined as "use intended by the provider".[34] This is used to classify whether a system poses a 'high-risk'[35] of harm to the health and safety or the fundamental rights of persons. Therefore, the 'intended purpose' affects the requirements of training, validation and testing of datasets[36] and its change requires a new conformity assessment.[37]

A related concept is that of 'reasonably foreseeable misuse', defined as the use of an AI system in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems.[38] Both the 'intended purpose' and the 'reasonably foreseeable misuse' form part of the risk management system required under Article 9 and the mandatory disclosure to users in terms of possible risks posed by a system.[39]

Notably, both concepts can only be applied to systems classified as high risk. For any other AI applications, no AI specific framework is established that would warrant their inclusion, leaving unregulated the misuse of any AI that is not classified as high risk. This is particularly worrying given that, as put forward in the proposal, misuse of AI technology can provide novel and powerful tools for manipulative, exploitative and social control practices, declared as particularly harmful and needing to be prohibited due to contradicting European Union values.[40]

The proposed framework also falls short when it comes to an AI system which is not classified in principle as high-risk but that can *begin* to create risks, of a varying degree, to health and safety or fundamental rights of persons as it is customised in the course of its use. Such concern applies particularly to general-purpose AI systems sold by tech companies which the buyer is free to develop further.[41] Even if a procedure existed for their assessment (despite the concerns raised in the above paragraph), it is dubious whether the 'intended purpose' – 'reasonably foreseeable misuse' dichotomy could capture such uses, which suggests that it needs to be supplemented with other categories of purpose and use.

BEUC recommendations:

- To enable assessment of systems other than those currently labelled as high-risk, the proposal must explicitly include a mechanism for evaluating purpose and foreseeable use, including misuse, for all AI systems. This mechanism should be

[33] Veale, Borgesius (2021) citing Harkin D, Molnar A, Vowles E. The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. Crime, Media, Culture. 2020;16(1):33-60. doi:10.1177/1741659018820562 https://journals.sagepub.com/eprint/XnAgFVFWyHGUv6dzbFPZ/full

[34] Article 3(12) of the proposal.

[35] Article 6(1) a) of the proposal.

[36] Recitals 43 – 44 of the proposal.

[37] Recital 66 of the proposal.

[38] Article 3(13) of the proposal.

[39] Article 13(3) b) iii) of the proposal.

[40] Recital 15 of the proposal.

[41] For an overview on automated machine learning systems ('AutoML', e.g. Google's Cloud AI AutoML, Amazon SageMaker Autopilot, Microsoft Azure automated ML) allowing business users the creation of customized machine learning models, see https://www.kdnuggets.com/2020/02/data-scientists-automl-replace.html (2020) and https://www.ibm.com/downloads/cas/RGN4EOZK (2019).

connected with the framework for classification of AI systems that should complement Article 6, as proposed in Section 6 below.

- To ensure the Regulation allows an accurate assessment of AI systems, the proposed mechanism for assessment must not be limited to the narrow notions of 'intended purpose' and 'reasonably foreseeable misuse' but should also allow the assessing body to examine 'potential use' or 'foreseeable use' of the given system.

4.6. Biometric data

The proposal uses the definition of 'biometric data' as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person."[42]

This is aligned with the definitions in other European Union legislation[43], but the way the definition is used here gives rise to concern.

This is notable when contrasting the use of biometric data as discussed in the context of biometric identification against the definitions of an 'emotion recognition system' (Article 2 (34)) or a 'biometric categorisation system' (Article 2 (35)) where the proposal also refers to the definition of biometric data. Applications using emotion recognition or biometric categorisation can nevertheless also operate using less detailed data than would be needed to perform or confirm identification of an individual, while still holding potential harm for consumers if deployed in commercial contexts, such as in-store emotion recognition systems.[44] In this vein, a system making inferences about consumers' emotions could escape classification as such under Article 2(34) by making a claim of not using biometric data – e.g. merely by virtue of using less data than would be required to establish or confirm a person's identity. This risk is embedded in the current wording's use of the term 'biometric data' which must be clarified.

BEUC recommendations:

- The definitions of 'emotion recognition system' (Article 2 (34)) and 'biometric categorisation system' (Article 2 (35)) should be amended to avoid being necessarily tied to the actual identification (or confirmation of an identification) of an individual. This way, a system making invasive (but anonymous) inferences about one's own emotional state or social category will not escape classification under Article 2 (34) or Article 2 (35).

4.7. Remote biometric identification systems

In the age of easily available and highly invasive facial recognition technology that can record and make inferences from a person's presence and movements in varying contexts, regulating the use of remote biometric identification systems is important.

Article 3 (36) defines a 'remote biometric identification system' as an AI system intended for the identification of natural persons at a distance, by comparing a person's biometric data with the biometric data contained in a reference database, and without prior knowledge whether the targeted person will be present and can be identified. 'Distance' is

[42] Article 3(33) of the proposal.

[43] Article 4(14) of Regulation (EU) 2016/679 of the European Parliament and of the Council, Article 3 (18) of Regulation (EU) 2018/1725 of the European Parliament and of the Council, and Article 3(13) of Directive (EU) 2016/680 of the European Parliament and of the Council.

[44] Vzbv (2021) Artificial intelligence needs real world regulation, https://www.vzbv.de/sites/default/files/2021-08/21-08-03_vzbv_Position_Paper_AIA_ENG.pdf, p. 9.

not explained and there is no mention regarding the targeted person's knowledge about being subjected to identification.

Two types of systems are distinguished:

- 'real-time' remote biometric identification systems, where the capturing of biometric data, the comparison and the identification all occur without a significant delay, ruling out limited short delays in order to avoid circumvention;
- 'post' remote biometric identification systems, meaning remote biometric identification systems other than the above.

Despite the attempt to rule out circumvention, the above definition still does not give a straight answer as to whether analysing a recording within hours of its creation is considered 'real-time', creating a risk of circumvention. Recital 8 is of little help, introducing terms of 'live' or 'near-live' material as well as that of a 'significant delay' described as "generated before the use of the system in respect of the natural persons concerned".[45]

BEUC recommendations:

- For a clear distinction of what constitutes a 'remote identification' system, the meaning of identification 'at a distance' as mentioned in the definition of Article 3(36) must be clarified.
- What constitutes 'real-time' and 'post' recognition as defined in Article 3(37)-(38), along with 'live' and 'near-live' material as mentioned in Recital 8 must be clarified.

5. List of prohibited practices (Article 5)

Article 5 establishes a list of four AI practices to be prohibited in the EU.

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 of Article 5 need to be substantially improved to effectively take into account consumers' interests and ensure both a broad and clear application of these prohibitions.

5.1. Subliminal techniques causing behavioural distortion and harm – Art. 5 (1) a)

The first prohibited AI practice consists of AI that deploys 'subliminal techniques beyond a person's consciousness to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm'.

First, we regret that the application of this provision is limited to AI that causes physical or psychological harm. AI that manipulates someone in a manner that causes him/her *economic harm* should also be included. This type of harm is a real risk in the age of dark patterns, even without the additional concerns brought by AI.[46] For example, price

[45] Recital 8 *in fine* of the proposal.

[46] A recent example demonstrates how manipulated interfaces have been found to push people into giving larger donations than they knew or planned to: https://www.nytimes.com/2021/04/03/us/politics/trump-donations.html

optimisation techniques, where insurance firms target price increases to those perceived as less likely to switch and/or more likely to pay should not be permitted, i.e. there should be no loyalty penalty for long-standing insurance consumers.[47]-[48]

Another example would be the use of smart meter data to establish personalised energy prices for consumers based on their consumption data. Suppliers could take advantage by adapting the price for electricity to the consumers' consumption pattern to make them pay more i.e. high electricity prices when your consumption is usually high. Our UK member Citizens Advice raised similar concerns in a recent report.[49]

Save for the narrowly defined case of social scoring conducted by or on behalf of authorities, *societal* harm has also been left out of Article 5, despite the clear reference to the need for such prohibitions in Recital 15,[50] and the clear indications of the harms caused by algorithmic ecosystems feeding on user attention and weaponization of polarizing content.[51]

Second, the wording 'in order to' limits the application of this provision to AI whose 'intended purpose' is to cause physical or psychological harm, thus excluding the 'potential use' or 'reasonably foreseeable misuse' of the AI.[52] Aside from whether the proposal allows the examination of intended purpose for systems other than high-risk,[53] we strongly reject the requirement to *prove intent. This* is not required in EU consumer law, in case of unfair commercial practices or product liability, and would be a significant and unacceptable step backwards regarding the level of protection that consumers need and are entitled to expect under EU law. It also would mean that these provisions are in practice unenforceable as it would be very difficult, if not impossible, to prove the original malicious intent.

Third, use of the 'subliminal' criterion, although undefined in the proposal,[54] means that a ban only applies to techniques which are barely noticed. As such, it is powerless in all cases where the individual has the faintest suspicion of being manipulated, leaving open situations where the individual is aware of the *presence* of algorithms but not of their *entire*

[47] The UK's Financial Conduct Authority and the Central Bank of Ireland have recently published market investigations show how insurers often engaging in price optimisation practices, specifically targeting price increases on consumers who are perceived as less likely to switch (a 'loyalty penalty'). These investigations were launched following research by our UK member Citizens Advice.

[48] For more information, read BEUC's position paper on Big Data and Insurance: https://www.beuc.eu/publications/beuc-x-2020-039_beuc_position_paper_big_data_and_ai_in_insurances.pdf

[49] https://www.citizensadvice.org.uk/a-price-of-ones-own-an-investigation-into-personalised-pricing-in-essential-markets/

[50] Recital 15 states: 'Aside from the many beneficial uses of artificial intelligence, that technology can also be misused and provide novel and powerful tools for manipulative, exploitative and social control practices. Such practices are particularly harmful and should be prohibited because they contradict Union values of respect for human dignity, freedom, equality, democracy and the rule of law and Union fundamental rights, including the right to non-discrimination, data protection and privacy and the rights of the child.'

[51] See e.g. European Parliamentary Research Service, Polarisation and the use of technology in political campaigns and communication, PE 634.414 – March 2019, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634414/EPRS_STU(2019)634414_EN.pdf, Reviglio U, Agosti C. Thinking Outside the Black-Box: The Case for "Algorithmic Sovereignty" in Social Media. Social Media + Society. April 2020. doi:10.1177/2056305120915613; https://journals.sagepub.com/doi/full/10.1177/2056305120915613; Bessi A, Zollo F, Del Vicario M, Puliga M, Scala A, Caldarelli G, et al. (2016) Users Polarization on Facebook and Youtube. PLoS ONE 11(8): e0159641. doi:10.1371/journal.pone.0159641 https://www.researchgate.net/publication/301926189_Users_Polarization_on_Facebook_and_Youtube; on creation of echo chambers see Cinelli, De Francisci Morales, Galeazzi, Quattrociocchi, Starnini (2021) The echo chamber effect on social media, Proceedings of the National Academy of Sciences Mar 2021, 118 (9) e2023301118; DOI: 10.1073/pnas.2023301118 https://www.pnas.org/content/118/9/e2023301118.

[52] See Recital 16 of the proposal.

[53] See section 4.5 on intended purpose and misuse.

[54] See the discussion in *Definitions* above.

functionality. Similarly, it leaves out an entire body of aggressive algorithmic techniques for choice manipulation which are deployed against individuals without any intention of being subliminal, such as choice architectures meant to evoke frustration and anger. Recent research shows that such techniques are highly successful despite the emotional price individuals pay for interacting with such systems.[55]

BEUC recommendations:

- Art. 5 (1) a) should be expanded to include AI practices that manipulates someone in a way that can cause them economic harm.

- Art. 5 (1) a) should be expanded to AI whose 'intended purpose' or 'reasonably foreseeable misuse' can manipulate someone and lead to physical, psychological or economic harm. This prohibition should also extend to uses which can be identified as 'potential use' or 'foreseeable use' and apply irrespectively of the risk classification of the AI system (see section 4.5).

- The 'subliminal' criterion of Art. 5 (1) a) should be removed as it is vague and unnecessary. The provision doesn't protect the consumer against aggressive behavioural manipulation in the digital environment which can be performed openly, causing the consumer a powerful emotional backlash and still delivering high rates of success in getting consumers to do something against their will.[56]

- A broad reversal of the burden of proof putting the onus of demonstrating compliance on the entity behind the AI system in all disputes involving individuals must be introduced in order to reinforce the prohibitions on manipulation.[57] This recommendation must apply across all prohibited AI practices mentioned in sections 5.2 to 5.6.

- Societal harm caused by an AI practice should also be included. In this regard, AI systems that manipulate someone in a way that can have an impact on the functioning of democracy and the rule of law should also be covered.

5.2. Vulnerability of groups – Art. 5 (1) b)

This provision focuses on AI that exploits 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.

First, it does not apply to AI used to exploit other types of vulnerabilities such as financial vulnerabilities. For example, an AI that exploits someone's gambling addiction in a manner that is likely to cause that person economic harm is allowed.[58]

[55] Luguri, Jamie and Strahilevitz, Lior, Shining a Light on Dark Patterns (March 29, 2021). 13 Journal of Legal Analysis 43 (2021) , University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 879, U of Chicago, Public Law Working Paper No. 719, Available at SSRN: https://ssrn.com/abstract=3431205 or http://dx.doi.org/10.2139/ssrn.3431205 at 65.

[56] id.

[57] See also section 7.6 on access to justice.

[58] Research shows how "*some in-game purchasing systems could be characterized as unfair or exploitative. These systems describe tactics that capitalize on informational advantages (e.g., behavioural tracking) and data manipulation (e.g., price manipulation) to optimize offers to incentivize continuous spending, while offering limited or no guarantees or protections (e.g., refund entitlement), with the potential to exploit vulnerable players (e.g., adolescents, problematic gamers).*"

Furthermore, while ensuring protection to the most vulnerable groups, this provision does not take into account the *permanent state of vulnerability of all individuals* created by exposure to 'black box' technology and economic practices that consumers cannot grasp.

The digital market is characterised by a profound imbalance of power, knowledge and agency, compared to other markets. This translates into a new position of vulnerability for consumers that is both structural (owing to the structure of digital markets which prevents consumers from interacting with market players on an equal footing) and architectural (due to the way interfaces are designed and operated). This imbalance and vulnerability are referred to in current academic debates as 'digital asymmetry'.[59]

Digital asymmetry is not addressed in the formulation of Article 5 (1) b), despite it being perpetuated and driven by algorithmic environments which use AI to maximise user monetisation and conversion rates. Current research suggests that the disempowerment of individuals in this context can only be addressed by a reversed burden of proof to prove a trader's compliance which must become the standard for all data-driven services addressed to consumers.[60]

Thirdly, the proposal does not take into consideration vulnerabilities of individuals which are not associated to their age, physical or mental disability. Consumers can become vulnerable for a temporary moment for different reasons (e.g. emotional distress, grief, sorrow, etc.). An AI system that takes advantage of that temporary vulnerability should also be prohibited.

Finally, similarly to Article 5 1(a), the wording 'in order to' ties the application of the provision to the construct of intended purpose of the AI system, as discussed earlier in this paper. This leaves out any considerations of 'potential use' or 'reasonably foreseeable misuse' of the AI. It also as raises a question about its applicability to non-high-risk systems where risk management, including its mechanism for evaluation of intended purpose, is not envisaged.[61]

BEUC recommendations:

- Art. 5 (1) b) should also apply to AI used to exploit vulnerabilities other than those related to children or of physically- or mentally-disabled people. For example, it should protect consumers made vulnerable through the use of persuasion profiles and personalisation practices (digital asymmetry) or through temporary vulnerabilities (e.g. grief, sorrow, emotional distress) who are not associated to group of people due to their age, physical or mental disability.

- Art. 5 (1) b) should be expanded to AI whose 'intended purpose' or 'reasonably foreseeable misuse' can manipulate someone and lead to physical, psychological or economic harm. This prohibition should also extend to uses which can be identified as 'potential use' or 'foreseeable use' and apply irrespectively of the risk classification of the AI system (see section 4.5).

[59] Helberger N. Lynskey O. Micklitz H.-W. Rott P. (2021) Structural asymmetries in digital consumer markets, BEUC, https://www.beuc.eu/publications/beuc-x-2021-018_eu_consumer_protection.0_0.pdf, at 46.

[60] Id, at 66 et seq.

[61] See section 4.5 on intended purpose and misuse.

5.3. Social scoring – Art. 5 (1) c)

While we welcome the prohibition of social scoring by public authorities, certain elements need to be clarified and the ban of this specific AI practice should be expanded to commercial use too.

Firstly, the use of social scoring by private entities is not explicitly regulated by the AI Act since it is not included in Article 5, nor is it in the list of high risk AI systems in Annex III.[62] This highly problematic gap must be addressed as social scoring by private entities can have a significant impact on our most basic fundamental rights and core democratic principles. It has been proven that people behave differently according to when they know that they are being observed or followed (the panoptic effect).[63]

For example, Airbnb recently patented an AI system capable of generating social scoring to determine consumers' trustworthiness based on a variety of social media/online data.[64] If operational, this AI is likely to lead to the discrimination of some social groups in the market for holiday homes – and yet, this may be just the tip of the iceberg.[65] Under the proposed rules, such an AI system would not be regulated by the AI Act.

Another controversial point is that the Commission's proposal seems to accept a discriminatory behaviour by means of social scoring if the detrimental or unfavourable treatment is proportionate to the individual's social behaviour (Art. 5 (1) I Subpoint (ii)).

Also, the prohibition of Article 5 I (i) is limited to social scoring that is based on data originally collected in a context that is unrelated to the context of the social scoring. In other words, scoring based on data originally collected in a context for social scoring would be lawful under the Commission's proposal.

For these reasons, and in line with the Opinion from European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS),[66] we support a general ban on the use of social scoring by both public and private entities.

BEUC recommendations:

Article 5 (1) c) should be amended as follows:

- It should include a general ban on AI used by both public and private bodies to evaluate the trustworthiness of an individual based on their social behaviour or other personal attributes, such as someone's preferences, emotions, health or intelligence.

- Social scoring should be prohibited regardless of the context under which the data used is collected.

[62] Although not explicitly mentioned, one could envisage the use of social scoring in AI used for education purposes under Annex III, Point 3.

[63] https://en.wikipedia.org/wiki/Panopticon

[64] Clark Boyd, Would You Pass the Airbnb Psychopath Test? Towards Data Science, January 12, 2020, https://towardsdatbiometricascience.com/would-you-pass-the-airbnb-psychopath-test-83e66cb55

[65] Christopher Mims, The Secret Trust Scores Companies Use to Judge Us All, Wall Street Journal, April 6, 2019, https://www.wsj.com/articles/the-secret-trust-scores-companies-use-to-judge-us-all-11554523206

[66] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021 https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf

- Discriminatory behaviour by means of social scoring should always be unlawful even if the detrimental or unfavourable treatment is proportionate in light of the individual's social behaviour.

5.4. Real-time remote biometric identification – Art. 5 (1) d)

Companies are increasingly using consumers' biometric data for different purposes. All over the world, facial recognition is used for 'tagging' people on social media platforms, to unlock smart phones or to authenticate/identify customers in the context of financial services. Biometrics are particularly sensitive data, and their illegitimate processing can have very serious consequences for consumers and society.

In a recent study[67] commissioned by the Arbeiterkammer[68], the Institute for Technology Assessment (Institut für Technikfolgen-Abschätzung) looked at the impact of the wide-scale use of biometric procedures on consumers. When it comes to facial recognition, the study underlined that it is a technology that, in today's terms, poses the greatest threat to fundamental rights and democracy. Due to technical shortcomings, such as extremely high error ratios, technically aggravated discrimination, racism, suppression, mass surveillance and the loss of privacy, anonymity and personal freedom, it should be regulated strictly.

Article 5 (1) d) forbids the use of 'real-time' remote biometric identification (RBI) systems in publicly accessible spaces[69] for the purpose of law enforcement (e.g. use of facial recognition AI on streets to scan passers-by).

However, this prohibition is not absolute. Under the current proposal, in certain situations (e.g. search for missing children) and under certain conditions (e.g. prior authorisation from judicial authority), the use of RBI systems in public spaces for law enforcement is permitted. The use of RBI by private entities is also allowed.

BEUC strongly disagrees with the approach taken in the proposal on this issue, particularly on the exclusive focus on RBI used by public authorities. Due to its inherent intrusiveness and the risk it represents for fundamental rights, core democratic principles and EU values, the use of remote biometric identification systems in public spaces by private entities must also be banned without exceptions.

This is also the position of the European Data Protection Supervisor and the European Data Protection Board which called for a general ban on any use of AI for automated recognition of human features in publicly accessible spaces, such as recognition of faces, gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals, in any context.[70]

As regards the use of remote biometric identification systems by public entities, the EU institutions should consider a full ban on such systems, in line with the recommendations of the EDPB and the EDPS.

[67] https://www.akeuropa.eu/policy-brief-body-access-key-biometric-methods-consumers

[68] Arbeiterkammer is an associated member of BEUC.

[69] Under the current proposal, 'publicly accessible spaces' means any physical place accessible to the public, regardless of whether certain conditions for access may apply (Art. 3 (39)).

[70] EDPB-EDPS Joint Opinion (2021), section 32 https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

BEUC recommendation:

- The use of remote biometric identification systems by private entities in public spaces should be banned, without exceptions.

5.5. Emotion recognition

The use of AI for emotion recognition is very worrying for consumers (e.g. real time facial recognition that analyses feelings and adapts what consumers see/or are offered accordingly) as it can lead to serious infringements of consumers' privacy and to their manipulation.

Furthermore, researchers have argued 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*'. [71]

Under the current proposal, AI used for emotion recognition is not considered to be of high risk and is simply subject to a transparency obligation.[72] This is not sufficient. The use of emotion recognition technology should only be allowed for strictly limited purposes and under very limited conditions, such as health or research purposes.[73]

BEUC recommendation:

- Article 5 of the AI Act should ban the use of emotion recognition AI except in very specific circumstances related to health or research purposes, in line with the recommendations of the EDPB and EDPS.

5.6. Scientifically unproven AI systems

Due to risk of fraud, as highlighted by Consumer Reports[74], the AI Act should also prohibit the placing on the market, sale and use of AI-enabled technology for which are not scientifically substantiated or have been debunked by science. A similar view was expressed in the joint opinion of the EDPB and the EDPS, calling for a prohibition of 'AI systems whose scientific validity is not proven or which are in direct conflict with essential values of the EU'.[75]

Examples include companies performing physiognomy (trying to use a person's facial features or physical characteristics to determine their character, personality or sexual orientation[76]) which is widely considered as pseudo-science, and other types of sentiment-analysis tools.

BEUC recommendations:

- The AI Act should prohibit the use of AI for which the scientific validity is unproven or the claimed benefits have been debunked by science.

[71] 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

[72] Article 52 of the proposal.

[73] EDPB-EDPS Joint Opinion (2021), section 35.

[74] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2660226_en

[75] EDPB-EDPS Joint Opinion (2021), section 33.

[76] https://mashable.com/article/artificial-intelligence-ai-lgbtq-gay-straight

6. Scope restriction and risk assessment

6.1. Scope restriction

6.1.1. High-risk systems

One of the main shortcomings of the proposal is the limited scope of application of its obligations and requirements. These almost exclusively concern ’high risk AI systems’, leaving a great majority of existing AI systems unregulated.

For any other AI system, the European Commission relies on the concept of voluntarism. The proposal suggests that the requirements for ‛high risk AI systems’ could be applied on a *voluntary* basis via codes of conduct, and their drawing up must be encouraged by the Commission and the Member States (Art. 69).

An AI system is considered high-risk if it is specified as such in Article 6 of the proposed Regulation, i.e. where it:

- constitutes a product or a safety component of a product covered by European Union harmonisation legislation listen in Annex II and requiring third-party conformity assessment, or
- is expressly listed in Annex III.

A high-risk AI system can be a safety component of a product which is not considered high risk under relevant harmonisation legislation.[77]

This approach has major implications. First, it leaves outside of the AI Act’s scope a vast majority of AI systems which affect the daily lives of citizens and consumers, such as online profiling and personalisation algorithms, content recommender systems that select what people see in their social media feeds.

Connected devices with AI embedded (e.g. smart meters, connected toys, virtual assistants) are not classified as high-risk AI systems. In this regard, there is a lack of clarity regarding the implications of Art. 43 (3) and the extent to which harmonised standards covering the requirements applicable to high-risk AI systems could also apply to what are considered ‛lower-risk’ connected devices.

Importantly, this approach does not address a multitude of risks for consumers which arise from their everyday activities in the digital sphere. Risk of harms related to use of e.g. algorithmic recommender systems and personalisation systems, must also be included (such as where an individual is only shown news items which aim to maximise engagement by evoking anger and despair). It should trigger an appropriate classification resulting in obligations such as duties of documentation (maintaining an audit trail) and reporting requirements.

Second, the approach leaves no room for flexibility to address other risks that may manifest themselves after an AI system’s deployment. Systems which for example begin to pose a high level of risk to fundamental rights[78] in the course of their operation such as general-

[77] Recital 31 of the proposal.

[78] This applies to e.g. the general-purpose AI systems discussed in section on intended purpose and misuse.the general-purpose AI systems discussed in section 4.5 on intended purpose and misuse.

purpose AIs,[79] cannot be included in its scope by any other means than by amending the Regulation or its Annexes. The AI Act runs the risk of becoming out of date very quickly.

Third, the 'high-risk' category is itself narrowly defined, excluding from its scope AI applications that can cause serious harm if misused. For example, AI systems intended to be used for underwriting and pricing purposes by insurance firms when offering insurance contracts to consumers are not considered 'high-risk' AI systems under Annex III.

The Low Voltage Directive[80] is not included in Annex II despite AI-powered consumer devices falling under its scope.

6.1.2. Updating the list of high-risk systems

The Commission intends to annually assess whether the list of high-risk applications in Annex III needs to be updated.[81] Unfortunately, such an update is subject to strict conditions that will make it very difficult to broaden its scope.

- First, the proposal limits the possibility to expand the scope to the areas already listed in Annex III (Art. 7 (1) a)). As the AI Act should be forward-looking, it is unreasonable to expect that AI, a technology of significant complexity and challenges, is not going to represent a high risk in other sectors than those currently mentioned in Annex III in the years to come.
- Second, AI can only be added to the scope of Annex III if it poses a risk of harm to the health and safety or has an impact on fundamental rights. This does not take into consideration the potential for economic harm or negative societal impacts.

6.1.3. Systems other than high-risk

BEUC is supportive of a 'risk-based approach' but one where all AI systems (including non-high-risk systems) are adequately regulated. For consumers harmed by an AI system, it is irrelevant whether the damage is created by a 'high-risk AI' or a lower-risk AI.

All AI systems, including medium- and low-risk, should be subject to a minimum set of common rules and principles. See Section 6 for an analysis of these principles.

BEUC recommendations:

- The scope of the AI Act should be broadened to adequately regulate AI systems other than those it currently classifies as 'high-risk', such as smart meters, AI-powered connected toys, virtual assistants or AI that organises what people see on social media.

- All AI systems employed in the EU, including medium- and low-risk systems, should respect a set of common principles established in the AI Act (e.g. transparency, fairness, non-discrimination).

- The existing list of 'high-risk' applications in Annex III should be expanded to include additional AI applications. For example, AI used to assess insurance premiums and AI payment and debit collection services. Also, the Low Voltage Directive should be included in Annex II.

[79] See footnote 41 for examples and further discussion on general-purpose AI.

[80] Directive 2014/35/EU on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits

[81] Articles 7(1), 73 and 84(1) of the proposal.

6.2. Assessment methodology to determine level of risk

The Regulation does not envisage a risk assessment test, or other means of classifying an AI system, that would complement the classification of ‘high-risk’. A process which determines the level of risk of an AI system (high, medium, low) and potential breaches of Article 5 should be introduced.

This process would take the form of a self-assessment by the provider of the system. This risk assessment should take into account numerous criteria, including the possible harms arising throughout the whole life cycle of the system for both individuals and society, the type and nature of the data used (e.g. personal / non-personal data); the harm for the environment, the intended use of the AI system; the type of algorithmic model, etc.

The purpose of such a risk assessment is two-fold:

- First, it will enable producers to classify an AI system under a specific risk category (high, medium or low) and to apply the rules/obligations that go along with that AI category before placing the AI system on the market or putting it to use.

- Second, this risk assessment should also determine whether the relevant AI system breaches any of the provisions of Article 5. If that is the case, it should be prohibited.

This risk assessment should be complemented with the conformity assessment procedure mentioned in Section 8 below.

BEUC recommendations:

- The risk framework must be broadened to also include categories of low and medium risk, to be assigned based on a risk classification system.

- The risk classification system must include a general clause that will allow classification of AI systems to assign them an appropriate risk category, from high-risk to low-risk.

- A preliminary self-assessment must be made mandatory to all providers of AI systems to determine the category of risk and to rule out breaches of any of the express prohibitions of Article 5 before the system is put into use at regular intervals after its deployment.

- The risk classification system should include risks in terms of health and safety, fundamental rights, consumer protection, economic harm, but also societal harms and the environment.

- Tiers other than high risk must also be subject to appropriate requirements, such as complying with the horizontal principles that the AI Act should establish (such as transparency and fairness)[82] and maintaining an audit trail (documentation duty) and reporting obligations for medium-risk systems to ensure an adequate and verifiable level of transparency.

[82] See section 7 below.

7. Horizontal AI principles and rights for consumers

Article 69 of the proposal encourages Member States to draw up codes of conduct to foster the voluntary application of the requirements set out in Title III, Chapter 2, to AI systems other than those considered high-risk. In addition to Article 52 on transparency and Article 5 on prohibited practices, only these voluntary commitments would be applicable to non-high-risk AI.

Given the significant risk and potential to cause harm that AI systems can pose for individuals and society, it is unacceptable to pin the protection of consumers on a set of non-enforceable rules.

As mentioned above, all AI systems should be subject to a set of binding horizontal principles (e.g. transparency, fairness, non-discrimination). Legal obligations and requirements should then gradually increase according to the level of risk. The greater the potential for an AI system to cause harm, the more stringent the legal requirements should be.

The horizontal principles must be translated into enforceable rights for individuals and obligations for business users and providers of AI systems.

7.1. Transparency, explanation, and objection

The AI Act establishes certain transparency obligations for 'high-risk AI systems', including transparency towards the users of the system[83] (i.e. for those who employ it, not consumers), supervisory authorities, documentation requirements. Article 52 also establishes limited transparency rules for certain AI.

However, there is no rule obliging providers or business users of an AI to provide an individual explanation of the specific reasons for a decision to those affected. Rules on transparency should be applicable to all AI.

Consumers should always have a right to receive an explanation about AI decision-making processes that may affect them individually or, on a larger scale, have the potential to cause harm to the society. Only with the right information can a decision be duly contested.

This right should encompass transparency about the fact that automation takes place[84], about how the AI system works, e.g. how information is processed and used, and what its purpose is, for example rank offers or tailor prices. Consumers should also have the possibility to request an explanation and learn how a machine has arrived at its result.

Finally, consumers should have a right to object to algorithmic decision-making and to request human intervention whenever a decision can have a significant impact on them. Such a right should exist regardless of whether the processing of consumer's personal data was involved in the algorithmic decision making.

BEUC recommendation:

- The AI Act should include a general principle requiring all AI systems to be used in a transparent manner in relation to citizens and consumers.

[83] Art. 13 of the proposal.

[84] Art. 52 of the proposal addresses this concern to a certain extent.

- The AI Act should enable consumers to always have a right to receive an explanation about AI decision-making processes that may affect them individually.

- The AI Act should give consumers a right to object to algorithmic decision-making and to request human intervention whenever a decision can have a significant impact on them.

7.2. Accountability and control

All AI systems must feature certain organisational and technical measures to ensure legal compliance and regulatory oversight. Article 14 establishes a system based on human oversight but, as with the majority of the proposal's requirements, it applies only to high-risk AI systems.

Whether an algorithm-based decision is accurate, fair, or discriminative can only be assessed if an appropriate control system is in place. There must be a minimum requirement that due control is exercised by the entity which has access to the AI's database and an understanding of how the decision criteria are selected and applied. The entity which deploys the AI system must monitor it on an ongoing basis. The higher the potential risks, the greater the accountability measures which must be put in place.

BEUC recommendation:

- The AI Act should include an obligation for all AI providers to regularly monitor the functioning of their AI system and assess if its respects the obligations and rights set out in the Act. Such control should always involve humans.

- The AI Act must include a general principle of accountability which clearly sets out that those entities that develop and use AI systems are responsible and must be able to demonstrate compliance with the law.

7.3. Fairness

AI systems must be developed and used in a fair and responsible way.

For example, decision-making processes must be fair from the perspective of the data that is processed, the means used in the decision process, and the intent behind the result. The outcome should be fair too, so as not to lead to unjust treatment or behaviour. The last aspect is not fully addressed by EU data protection law, which focuses on the fair processing of personal data, but not on the consequences resulting from inferences and predictive analysis.

Questions of fairness should also be seen under the aspect of general welfare considerations. A lack of fairness can lead to even greater societal asymmetries, unequal benefits for citizens/consumers, or could even lead to certain groups of people being exposed to higher risks of poverty. The deployment of AI systems must be accompanied by an assessment of their impact on the well-being of citizens.

BEUC recommendation:

- The AI Act should include a general principle that all AI systems and AI practices must be fair to individual citizens/consumers and society.

7.4. Non-discrimination

Consumers should be protected from illegal discrimination and unfair differentiation through the use of AI systems.

Through use of biased datasets and algorithms, a profiling process may conduct erroneous inferences and produce incorrect predictions, wrongly classifying individuals by assuming certain characteristics. When aggregated, such errors could disproportionately harm certain groups.

Many situations cannot be properly tackled using existing anti-discrimination laws, as these traditionally focus on discrimination based on typical protected characteristics, such as race. Instead, AI systems can use categories to differentiate between groups that are not (directly) related to such characteristics.

A prohibition on discrimination is included in Article 21 of the European Charter of Fundamental Rights (ECFR), featuring an open-ended list of parameters such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation. The risk of discrimination was also the reason the EPDB and EDPS recommended a prohibition on AI systems conducting biometric categorisation of individuals.[85]

The proposal should prohibit AI systems from enabling or allowing discrimination of individuals on the basis of the characteristics listed in the Charter, on the basis of biometrics or otherwise. It should also include other types of unfair discrimination such as that based on economic factors. Without including this principle, consumers will not be adequately protected against the risk of discriminatory AI systems.

BEUC recommendation:

- The AI Act should impose on all AI providers and business users a general obligation of non-discrimination. This should include a prohibition on AI systems which lead to discrimination on the basis of the characteristics specified in Article 21 European Charter Fundamental Rights, based on biometric data or otherwise, but also unfair discrimination based on economic factors.

7.5. Safety and security

All AI-powered products and services must be safe and secure throughout their lifecycle.

In addition to the necessary measures in relevant product-specific legislation, such as the EU directives on product safety and NLF (New Legislative Framework)-based legislation, it is important that the AI Act establishes a horizontal safety and security principle for all AI systems. This is particularly important given that AI systems are increasingly integrated in all types of products and services. It is also coherent to establish such a principle in the proposed Regulation, given its prominent focus on safety related issues.

BEUC recommendation:

- The AI Act must include a general principle requiring AI-powered products and services are safe and secure throughout their lifecycle (‘security by design and by default’).

[85] EDPB and EDPS Joint Opinion, Section 33.

7.6. Access to justice and right to redress, including collective redress

Greater protection in terms of transparency, safety, non-discrimination, or fairness are vital before consumers can trust AI-powered products and services. However, it is equally important to ensure that consumers have access to justice if AI-associated risks materialise. Victims should have a right to redress if harm occurs.

The AI Act proposal completely fails to address this point. It does not include any mechanism allowing consumers to use private enforcement tools when an AI system or practice infringes their rights or causes them harm.

The proposed Regulation cites the assurance of effective redress as one of the reasons to classify the use of certain AI systems by law enforcement authorities as high-risk.[86] The Explanatory Memorandum also makes a reference promising redress to be 'made possible' in the context of infringements of fundamental rights.[87]

Despite this, redress mechanisms do not exist in the proposed Regulation and individuals are not granted any instruments to protect their rights against infringements.

There is no right to complain to a national supervisory authority or an obligation for companies to provide for a complaint mechanism. For example, if a consumer is harmed by non-compliant high-risk AI system or by an AI practice prohibited under Art. 5, the proposed rules do not foresee any rights or mechanisms to obtain redress. In consequence, the party which is the most vulnerable to harms caused by AI (the individual) is also the least protected.

Also, the proposal does not allow civil society organisations, including consumer organisations, to represent harmed consumers in the exercise of their rights. An article akin to Art 80 GDPR (Representation of data subjects) is missing.[88]

In addition to allowing consumers to mandate consumer organisations (or other civil society organisations where relevant) to represent them individually, the AI Act must allow representative actions to be used to defend consumers' rights collectively. This should apply in the case of illegal commercial practices, or in obtaining compensation in case of harm suffered by a group of consumers. Consumers must be able via consumer organisations to jointly bring a court case to obtain compensation for damages arising from the same source (e.g. multiple consumers harmed by the same non-compliant AI system). They must also be able to ask the court to issue an injunction and stop the illegal practice. Consumer organisations must therefore be able to bring collective actions against AI systems and practices. The Representative Actions Directive[89] must apply in this area.

In the absence of adding the AI Act to the RAD Annex I, consumers would have no way of exercising their rights collectively. Given the huge asymmetry of information and the vulnerability of consumers most AI cases will involve, it is unlikely they will ever be able to bring court cases individually. Representative actions are their only realistic possibility to seek justice.

[86] Recital 38 of the proposal.

[87] Explanatory Memorandum, Section 3.5 Fundamental rights.

[88] Article 80 GDPR enables consumers to mandate a not-for-profit body to lodge complaints on their behalf.

[89] Directive (EU) 2020/1828 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC

To enable collective actions, the AI Act needs to be included in the Annex of the Representative Actions Directive. Such a provision was included in the recent Commission's proposal for a Digital Services Act.

BEUC recommendations:

The AI Act should include:

- A right for consumers to complain to a national authority or launch a legal action in court when an AI system or practice which affects them infringes the Regulation. This should include a right to receive compensation for material or non-material damages suffered.

- An obligation for companies to make a complaint mechanism available to consumers. Companies must be obliged to react to those complaints within a short period of time.

- An article allowing consumer organisations or more broadly civil society organisations to represent individual consumers in the exercise of their rights under this regulation. They should also be allowed to act in the 'general interest' (i.e. be able to bring forward complaints without a mandate from an individual, when they consider that an AI system or practice is infringing the rules).

- A provision that adds the AI Act to the Annex of the Representative Action Directive (RAD), which lists the laws where it is possible to file a representative action. It must be possible to file collective redress or injunctive actions in case of non-compliant AI.

7.7. Reliability and robustness

AI-powered products must be technically reliable and robust by design.

The more autonomous machines become, the more important it is for users to trust the system's reliability regarding their performance, accuracy, and robustness throughout their life cycle.

High quality data is essential for machine learning solutions. Requirements and guidelines on data quality are necessary to ensure that AI systems perform the intended functions. In this respect, companies must use proper training data sets and put data quality mechanisms in place to avoid biases, errors, and other irregularities. Review and validation processes should become a common industry standard.

BEUC recommendation:

- The AI Act should introduce a general principle that the performance of AI systems must be reliable, accurate, and robust throughout their life cycle.

8. Conformity assessment procedure (Art. 43)

The proposal relies far too much on industry self-assessing its compliance. With third party assessments carried out in only rare cases, this approach is inadequate as it does not take into consideration the complexity of the risks posed by AI.

First, consumer trust on AI powered products and services is likely to be stronger if the conformity assessment procedure is carried out by a third party.

Also, the proposed framework will lead to conflict of interest: the entity assessing whether a certain product is in compliance with the rules is the same which is trying to place the AI on the EU market as quickly as possible.[90]

Self-assessment should not be the default rule when it comes to conformity assessment procedures. While this conformity assessment procedure can be used for 'low-risk AI', it must not be used for 'high-risk AI'.

BEUC recommendations:

- Third party assessment should be the rule to assess the conformity of 'high-risk AI systems'. Self-assessment should only be allowed in when AI systems are not considered to be high-risk.

- For high-risk AI systems, the results of the conformity assessment procedure and all relevant documentation (including the results of the self-assessment foreseen in Section 6.2) must be notified to the relevant market surveillance authority before the product is placed on the market and published in a publicly accessed database.

- For non-high-risk AI systems, the results of the conformity assessment procedure and all relevant documentation (including the results of the self-assessment foreseen in Section 6.2) should only be notified to public authorities when they have requested it.

9. Standards (This chapter is co-authored by ANEC[91] and BEUC)

According to the concept of the proposed AI Act, the successful application of the AI Act will heavily depend on the development and application of harmonised (technical) standards by the manufacturers of an AI system. Although the New Approach of 1985 and the later New Legislative Framework, both making reference to harmonised standards, have proved key in building the Single Market for Goods, we are far from convinced that a regulatory tool designed to facilitate market access is the correct tool to protect the fundamental rights of consumers in the domain of AI.

Article 40 establishes a strong incentive for the application of standards by manufacturers: high-risk AI systems which are in conformity with harmonised standards are presumed to be in conformity with the requirements of the AI Act, thus inversing the burden of proof about the compliance of the legal requirements. Another incentive for the use of standards lies in Article 43, according to which service providers of an AI system who have applied harmonised standards will be able to carry out a self-assessment.[92]

The heavy reliance of the proposed AI Act on harmonised standards and on the standardisation process to regulate AI, and therefore in using this tool to ensure that fundamental rights and the required level of consumer protection are granted, raises serious concerns and is an essential flaw of the proposed AI Act.[93]

[90] A survey about independent third-party testing from International Federation of Inspection Agencies (IFIA) shows that the compliance and safety of independently-checked products is considerably higher than for products that rely simply on manufacturer's self-declaration of conformity.

[91] https://www.anec.eu/

[92] See section 8 for more information on the conformity assessment procedure.

[93] Several academics and organisations have explained in detail how the use of standardisation can undermine the EU's democratic process. See Michael Veale, Frederik Zuiderveen Borgesius (n 8); Martin Ebers,

First, it is not at all clear how fundamental rights and EU values and principles can be adequately transposed into technical standards. Despite the fact that in many international fora, standardisation of AI is high on the agenda and many initiatives have been undertaken already[94], for the EU, this must not be the only way to establish trustworthy and human-centric AI.

It is not the role of standards to interpret legal requirements but that of a democratic legislative procedure. Technical standards must *not* go beyond the implementation of mere technical aspects and enter in areas of public policy and law which require a certain level of interpretation. [95]

Concretely, under the proposed AI Act, it is unclear how technical standards will help service providers determine, for example, what types of biases are prohibited and how they should be mitigated (Art. 10 (2) f)).

The way the AI Act envisages the role of standards amounts to a *de facto* regulation by private bodies (‘regulatory capture' phenomenon) and thus a serious lack of democratic accountability. [96] An Advocate-General from the Court of Justice of the European Union has already referred to standardisation as "*legislative delegation in favour of a private standardisation body*".

As we are in the presence of a double delegation of powers (from the co-legislators to the Commission and then from the Commission to the European Standardisation Organisations) in the field of fundamental rights, it is essential that the AI Act clearly ringfences the conditions under which such delegations take place.[97]

Secondly, civil society and consumers' interests are not sufficiently represented at national, European and international standardisation bodies. These bodies are essentially driven by industry. The influence of consumer organisations is limited because of a lack of resources and expertise at the national level, and the setup of decision-making process (based on the national delegation principle).

Finally, from the European perspective, the increasing push of industry, reflected by the National Standardisation Bodies members of the European Standardisation Organisations, to set a single, globally-relevant standard is encouraging a convergence between European and international standards. Given the primacy of international standardisation over the regional, the consequence is that more standards for application within Europe are being drafted or revised at international level. However, the participation of consumers and civil society is even more limited in international standardisation discussions, while there is a

Standardizing AI – The Case of the European Commission's proposal for an Artificial Intelligence Act, in: Larry A. DiMatteo/Michel Cannarsa/Cristina Poncibò (eds.), The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics, pending for publication, 22 pages, Cambridge University Press 2022;

[94] https://ethicsinaction.ieee.org/p7000/

[95] As highlighted by Martin Ebers (n 110) "The standardization of AI systems is not a matter of purely technical decisions. Rather, a series of ethical and legal decisions must be made, which cannot be outsourced to private SDOs [Standard Developing Organisations], but which require a political debate involving society as a whole." ANEC comments on the European Commission proposal for an Artificial Intelligence Act (ANEC-DIGITAL-2021-G-071)

[96] Ebers (n 110)

[97] Opinion of AG Campos Sanchez-Bordona in case C-613/14 James Elliott ECLI:EU:C:2016:63 [55] James Elliott ECLI:EU case C-613/14: ‘it must, moreover, be noted that while the development of such a harmonised standard is indeed entrusted to an organisation governed by private law, it is nevertheless a necessary implementation measure which is strictly governed by the essential requirements defined by that directive, initiated, managed and monitored by the Commission, and its legal effects are subject to prior publication by the Commission of its references in the ‘C' series of the Official Journal of the European Union.

strong participation of countries that do not share European values and principles, especially in AI standardisation.

The use of standardisation as proposed in the AI Act is unacceptable in a field as sensitive and fundamentally important to our society, and to the fundamental rights of individuals, as AI, particularly bearing in mind the EU's objectives for the digital transition. More detailed and clearer requirements are needed in the AI Act for standards to function as 'technical specifications for repeated or continuous application'[98] and not to have the role of determining the level of protection of fundamental rights and thus possibly restricting such rights.

BEUC recommendations:

- Harmonised standards must not be used to define or apply fundamental rights, legal or ethical principles. Their use should be limited to implement technical aspects. In this regard, a standard should, for example, not be used to determine what types of biases are prohibited under Art. 10 (2) f). Instead, the AI Act must include more detailed rules about the requirements applicable to 'high-risk AI', including rules on discrimination.

- As standards will play an important role to detail the essential requirements listed in the AI Act, the governance system of the standardisation process must be changed significantly. Consumer organisations must be systematically involved in standardisation. Public authorities must also provide the political and financial frameworks that permit the participation of all stakeholders – including consumers and broader societal interests. A general change of the standardisation process cannot be done overnight, but new Articles should be added to the AI Act to cater for such participation.

- Given that public authorities have also withdrawn from many standardisation activities to the detriment of the public interest, we call on authorities to become more engaged in standardisation and support consumer participation in it.

10. Enforcement

10.1. Reporting (only) of serious incidents and of malfunctioning of high-risk systems (Article 62)

Under Article 62, providers of high-risk AI systems placed on the European Union market are to report to market surveillance authorities a "serious incident or any malfunctioning of those systems which constitutes a breach of obligations under Union law intended to protect fundamental rights".

It should be clarified in a Recital that a breach of consumer rights would fall under the obligation to report under Article 62. As such, a company should be obliged to report a faulty AI used in an energy distribution grid for example, which can have a serious impact on the finances and wellbeing of consumers by inadvertently cutting off their energy supply or overcharging them.

An important aspect that is also missing in Article 62 is the obligation to notify those subject to the AI system, i.e., consumers, regarding a serious AI incident or malfunctioning AI.

[98] Art 2.1 Regulation 1025/2012 on European Standardisation,

The establishment of a culture of information-sharing and cooperation is key to increasing trust in the market and ensuring a high level of consumer protection.

BEUC recommendations:

Article 62 must include the following:

- A Recital must clarify under Article 62 the obligation to report a serious incident includes breaches of consumer rights.
- Article 62 must ensure that consumers affected by a serious AI incident or malfunctioning should be immediately informed about it.

10.2. Governance structure and enforcement (Article 63)

The proposed governance structure rests mainly at national level with market surveillance authorities. While this methodology has been regularly used in New Legislative Framework laws, its replication in the AI Act raises several concerns in relation to the obligations, competences and powers of the different actors involved and the different processes envisaged.

First, there will be many different national authorities responsible for overseeing the application of the AI Act. For example, for AI systems listed in Annex II – Section A, the authorities responsible for that product safety legislation will be competent.[99] For some AI systems listed in Annex III, Member States will have to designate a competent authority.

This raises the following concerns:

- The enforcement of the AI Act will greatly depend on the resources allocated to these different authorities. As it stands, data and consumer protection authorities may only play a marginal role due to the limited scope of Annex II and the competence under NLF based frameworks. The governance structure should clarify that where consumers interest (other than safety) are affected, or consumers are concerned as data subjects, these authorities should have access to relevant documentation and can require testing and investigations.
- However, the myriad of competent authorities under the AI Act (e.g. consumer protection authorities, telecommunications authorities, etc.[100]) will make it harder to ensure that each of these authorities has the adequate financial and human resources or the technical expertise to address the challenges of AI systems (Article 59 (4) of the proposal).
- To address possible shortcomings in terms of resources, enforcement at national level should be reinforced on a technical level by a highly specialised body of technical experts established by the Commission. This body should be tasked on a case-by-case basis with conducting expert evaluations and assessments of AI systems on request of a national authority conducting an investigation, in order to issue an opinion that is non-binding on the national authority. For cost efficiency, a single such body could be established at EU level and assist national authorities in the technical aspects of their investigations, to the extent indicated in their specific requests.

[99] Article 63 (3) of the proposal.

[100] As an example, these are the authorities competent for the application of the Radio Equipment Directive, which is one of the legal acts mentioned in Annex II – Section.

- The number of authorities involved in the application of the Regulation raises concerns regarding the effectiveness and consistency of the enforcement and oversight system when it comes to the cooperation between the different competent authorities and supervisory authorities at national level and cross borders. This is why it is very important that enforcement cooperation between national authorities becomes an official task of the AI Board (see section 10).

Second, while the Commission plays a central role if a national supervisory authority notifies its intention to adopt measures concerning an AI system in its territory[101], the Commission has no powers to proactively take the lead in case of inaction by national authorities. In this regard, the procedure foreseen in Article 66 should not be limited to actions started by Member States' authorities. The European Commission should be able to start an evaluation procedure about an AI system according to Article 66 whenever (i) it has sufficient reasons to believe that that an AI system presents a risk,(ii) no market surveillance authority started an investigation under Article 65 (2) and (iii) the AI system affects consumers in more than one Member State.

Thirdly, as already mentioned by other stakeholders[102], one point that has not been addressed in the proposal is the possible overlap between the competences of national supervisory authorities under the AI Act and the competences of other authorities, such as the data protection authorities under the GDPR. The AI Act must clarify to whom consumers can complain in situations of overlap and who takes the lead in the enforcement action. There must be a clear and coherent oversight and enforcement structure to guarantee cooperation among all relevant authorities and the effective and consistent protection of consumers across the EU.

Crucially, the precautionary principle[103] allows market surveillance authorities to take temporary and preventive measures in the absence of proof of harm to consumers. As such, we deplore that this fundamental principle is absent from the AI Act.

This principle should be applied where scientific evidence is insufficient, inconclusive or uncertain, and preliminary scientific evaluations indicate that there are reasonable grounds for concern. We consider it essential to ensure that technologies that pose significant harms for individuals and society are not deployed until they are tested and certified.

BEUC recommendations:

- Enforcement at national level should be reinforced on a technical level with the creation of a highly specialised body of technical experts designated by the Commission. Such a body should assist national authorities and the Commission in the technical aspects of their investigations and have the competence to issue non-binding opinions about specific cases brought up by the national authorities.

- The procedure foreseen in Article 66 should not be limited to actions started by Member States' authorities. The European Commission should be able to start an evaluation procedure about an AI system under this provision whenever (i) it has sufficient reasons to believe that that an AI system presents a risk, (ii) no market surveillance authority started an investigation under Article 65 (2) and (iii) the AI system affects consumers in more than one Member State.

[101] Articles 65 (5) and 66 of the proposal.

[102] https://www.accessnow.org/eu-minimal-steps-to-regulate-harmful-ai-systems/

[103] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52000DC0001&from=EN

- The AI Act must clarify that market surveillance authorities carry out their activities based not only on proportionality but also on a precautionary approach.

10.3. Access to data and documentation (Art. 64)

It is important that third parties such as consumer organisations or other civil society organisations have access to relevant documentation created in the context of this proposal by the AI provider (including the results of the conformity assessments as well as all relevant documentation foreseen in section 8).

BEUC recommendation:

- Article 64 should grant consumer organisations the right to access relevant documentation created in the context of the AI Act by the provider and request the authority to carry out ad-hoc audits of a particular AI system.

10.4. Procedure for dealing with AI presenting a risk at national level (Art. 65)

When it comes to non-high-risk systems, the application of Article 65 lacks clarity and consistency.

Article 65 (1) appears to establish a framework for assessing risk at national level, referencing Article 3 (19) of Regulation (EU) 2019/1020 on market surveillance, offering that a 'risk' is to be "*understood as a product presenting a risk defined in Article 3, point 19 of* [Market Surveillance Regulation] *insofar as risks to the health or safety or* […] *fundamental rights of persons are concerned*". This formulation is unclear but it would appear its role is to enable a generally applicable risk assessment[104] but limited to health, safety and fundamental rights.[105]

According to Article 65 (2), when a market surveillance authority has 'sufficient reasons' to believe that any AI presents such a risk to health or safety or to the protection of fundamental rights, assessed in accordance with Article 65 (1), it must carry out an evaluation of the AI in respect of its compliance with all the requirements and obligations of the AI Act.

However, the reference to the compliance with the requirements and obligations of the proposal is misleading as the Regulation establishes very few obligations for non-high risk AI systems. The only area where a non-high-risk AI system would be covered by this provision is a breach of the Article 5 'black list' (which will be extremely rare) or transparency obligation of Article 52.[106] In all other cases, the provisions of Article 65 (2) only allow the national authority to launch an investigation into high-risk AI systems.

Also, to ensure that the evaluation carried out by the market surveillance authority does not significantly delay the enforcement process, Article 65 (2) should clarify that this evaluation should be concluded without undue delay and should never take longer than 6 months.

[104] i.e. going beyond that considered reasonable and acceptable in relation to its intended purpose or under the normal or reasonably foreseeable conditions of use of the product concerned, including the duration of use and, where applicable, its putting into service, installation and maintenance requirements - Art. 3(19), Market Surveillance Regulation.

[105] See also the comments on structure of risk in Section 4

[106] This applies to AI systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content (Article 1(c)).

When it comes to the notification to other Member States of the application of corrective measures to an AI system, in addition to the rules foreseen in Article 65 (2),[107] market surveillance authorities should be obliged to inform other Member States when, during the course of their own evaluation, there is credible evidence that the AI system under investigation may also harm consumers in other Member States.

The proposal does not put in place a mechanism requiring early cooperation between national authorities from different MS when investigating suspicious AI systems. If a national authority starts an evaluation of an AI system under Article 65 (2), the AI Act does not foresee any obligation for this authority to notify it to the national authorities from other Member States. There could then be a situation where authorities from different Member States are investigating the same AI system in parallel without any cooperation or coordination. While in practice this issue may be addressed by the European Artificial Intelligence Board, it is important to ensure a coherent and consistent application of the AI Act by specifying in Article 65 (2) that authorities which start an investigation into a suspicious AI system must inform their counterparts in the other Member States within the AI Board.

Finally, civil society organisations should have the right to request an evaluation of AI systems by notified bodies when there are reasonable indications that the AI system causes significant harm.

BEUC recommendations:

- Civil society organisations must have the right to request an evaluation of AI systems by notified bodies when there are reasonable indications that the AI system causes significant harm.

- The wording “sufficient reasons to consider” under Article 65 (2) should be clarified to avoid misunderstanding and uneven application at national level. In any case, a complaint from consumers should be considered as sufficient reasons to launch an investigation by the market authorities under Article 65 (2).

- To ensure that the evaluation carried out by the market surveillance authority does not significantly delay the enforcement process, Article 65 (2) should clarify that this evaluation be concluded without undue delay and never take longer than 6 months.

- To ensure a coherent and consistent application of the AI Act, the Act must specify in Article 65 (2) that authorities which start an investigation into a suspicious AI system must inform their counterparts in the other Member States within the AI Board.

- As indicated in section 6, the requirements of Article 6 for high-risk systems must be complemented with a common framework of rules and obligations applicable to AI systems presenting medium or low risk, along with a flexible system that would allow authorities and regulators to actively assign risk categories to AI systems. Once this is achieved, the wording of Article 65 (2) will be clearer as it will allow actual assessments of risk presented by an AI system.

[107] According to Article 65 (5), market surveillance authorities shall inform the Commission and other Member States about any corrective measures applicable to a non-compliant AI system.

- The risks mentioned in Article 65 (1), as in the case of the entire Regulation, should not be limited to health, safety and fundamental rights[108] but also include economic harm or societal impacts.

- The wording of Article 65 (1) must leave no doubt regarding which parts of Article 3 (19) of Regulation (EU) 2019/1020 on market surveillance are included by reference.

10.5. Union Safeguard Procedure (Article 66)

Under Article 66, when objections are raised by a Member State against measures taken by another Member State or when the Commission considers that certain measures are contrary to EU law, the Commission shall enter into consultation with the relevant Member States and start an evaluation.

BEUC supports the European Commission's involvement in these types of cross-border procedures. We regret however that the Commission was only given the power to accept or refuse the measures taken by a Member State. The Commission should also be able to propose alternative measures to those taken by the authority of the Member State that initiated the procedure under Article 65, after seeking the advice of the AI Board.

BEUC recommendation:

- The Commission should be able to propose alternative measures to those taken by the authority of the Member State that initiated the procedure under Article 65, after seeking the advice of the AI Board.

11. AI Board (Articles 56 – 58)

The proposal establishes a European Artificial Intelligence Board ('AI Board') composed of representatives of the Member States, the European Data Protection Supervisor and the European Commission. The Board contributes to effective cooperation between national authorities.

The autonomy and powers of the European AI Board, comprised of high-level representatives of the national supervisory authorities and chaired by the Commission, seem limited regarding the application and enforcement of the AI Act.

One of the AI Board's specific tasks should be to ensure that market surveillance authorities cooperate in the enforcement of the AI Act. The adequate functioning of Articles 65 (Procedure for dealing with AI systems presenting a risk at national level) and 66 (Union Safeguard Procedure), a crucial part of the enforcement mechanism of the AI Act, will heavily depend on a smooth cooperation between the different national supervisory authorities. It is therefore of the outmost importance that the AI Board discusses and assesses the functioning of these provisions and if there is a need to improve their application.

[108] See comments in Section 4.3.

BEUC recommendation:

- The tasks of the AI Board must include ensuring that market surveillance authorities actively cooperate in the enforcement of the AI Act, particularly in the application of Articles 65 and 66.

12. Interplay with other areas of EU laws

12.1. General Data Protection Regulation (GDPR)

Existing data protection legislation, in particular the GDPR, plays an important role in the regulation of AI. In this regard, as pointed out by the EDPS and the EDPB, the Act must explicitly state that the GDPR applies to any processing of personal data falling within the scope of the AI Act, and that its provisions are without prejudice to the rights and obligations established under the GDPR.

However, the GDPR does not provide sufficient protection in an AI context. Key rights for consumers, such as the right to contest an algorithmic decision[109], should not depend on the processing of personal data as this is the case under EU data protection rules.

12.2. Product Liability Directive (PLD)

In parallel and as a complement to the AI Act, the European Commission is considering updating civil liability rules to cope with the challenges brought by AI, which include limited predictability, autonomous behaviour, continuous adaptation, complexity and opacity making difficult for claimants to claim compensation in case of harm.

There is still uncertainty about the instrument that the Commission will propose. This may either be done through a revision of the Product Liability Directive and/or a specific instrument laying down civil liability rules for AI based on their risk profile. The European Commission published its inception impact assessment on the review of the Product Liability Directive on 30 June and the consultation period is now ongoing. The Commission is expected to publish its proposal in the fourth quarter of 2021, or the first quarter of 2022.

BEUC strongly supports a revision of the Product Liability Directive. Adopted 36 years ago, this legislation is now outdated to cope with the problems arising out of (in particular) in the digital context.[110] During this time, many 'offline' products have since been replaced by digital goods. In order to fight the strong information asymmetries preventing consumers from claiming compensation, there should be a reversal of the burden of proof for plaintiffs.

12.3. Medical Devices Regulation

The proposal explains that the compliance of a high-risk AI system with its requirements will also be reviewed as part of the conformity assessment under the existing Medical Device Regulation (MDR) and will be 'CE' marked before being placed on the market. Therefore, the CE marking will be an indication of the product's compliance with the MDR as well as with the AI Act.

[109] Article 22 General Data Protection Regulation.

[110] https://www.beuc.eu/publications/product-liability-20-how-make-eu-rules-fit-consumers-digital-age/html

However, the AI Act proposal does not spell out the interplay between its requirements and the regulatory obligations deriving from the MDR. On one hand, the MDR imposes detailed requirements regarding the development and marketing of medical devices at each stage – design and development, risk management, quality management, post marketing activities and so on. On the other hand, the proposed AI Act specifies the provider's and (business) user's obligations at these stages as well. It remains unclear how these two sets of regulatory requirements will combine into one regulatory process without overlapping or creating interpretation issues. There needs to be further examination and perhaps a tailoring of regulations to implement the proposed AI regulatory requirements properly in the medical field.

12.4. AI and consumer law – Addressing digital assymetry

AI systems are instrumental in creating and perpetuating an ongoing state of asymmetry in the digital consumer-trader relationship. AI leads to further consumer disempowerment.

The trader has a real-time influence on the environment the consumer finds himself, including its choice architecture. Traders also have access to the consumer's detailed personal profiles, including decision-making biases and pressure points.

AI-driven algorithmic personalisation of interfaces and content adds a level of efficiency to user monetisation and conversion rates.[111] This translates into a new position of vulnerability for consumers that is both structural (owing to the structure of digital markets which prevents consumers from interacting with market players on an equal footing) and architectural (due to the way interfaces are designed and operated). This imbalance of power and the embedded vulnerability are referred to in current academic debate as digital asymmetry[112] and must be addressed through a review of the EU consumer law acquis.

A review must introduce new measures such as a modernisation of the concepts of 'fairness' and 'vulnerability', the expansion of blacklisted practices to include 'digital' practices and the introduction of a reversal of the burden of proof, placing the onus on the trader to prove their compliance with relevant legislation.[113]

12.5. AI and sustainability

Digitalisation and AI can help the urgently needed green transformation and the move towards more global sustainability. But they can also act as a 'fire accelerant' if not managed properly. To this end, the connection between the carbon footprint and computer processing is another of the essential considerations to be made when regulating AI. However, as explained previously,[114] one of the drawbacks of the risk classification adopted in the proposal is that no assessment framework is proposed that would allow authorities to evaluate the impact of an AI system on fundamental rights, including the right to a high level of environmental protection.[115]

Empirical findings have shown that digital technologies contribute to 4% of overall greenhouse gas emissions, a number expected to double by 2025.[116] Other studies show that training a single AI model emits carbon dioxide in amounts comparable to that of five cars over their lifetimes This problem must not be underestimated, particularly in the

[111] Helberger N. Lynskey O. Micklitz H.-W. Rott P. (2021) Structural asymmetries in digital consumer markets, BEUC, https://www.beuc.eu/publications/beuc-x-2021-018_eu_consumer_protection.0_0.pdf, at 106.

[112] Id, at 46.

[113] Id, at 48, 75.

[114] See section 4.3 on risk.

[115] Article 37 of the EU Charter of Fundamental Rights.

[116] Maxime Efoui-Hess, *Climate Crisis: The Unsustainable Use of Online Video*, Shift Project (2019).

context of the European Green Deal. In this sense, there needs to be a general rethink of political strategies to ensure coherence between sustainability and digital policy objectives. For example, it is contradictory to push for a massive use of IT systems that require infrastructures that are potentially very energy/carbon intensive without adequate measures to control their environmental impact.

12.6. AI and financial services

Insurers have always collected consumer data to inform their pricing and underwriting decisions when offering insurance contracts. However, the growing use of Artificial Intelligence and Big Data Analysis is transforming the sector, allowing insurers to process larger sets of data about consumers (including new, non-traditional data) and to price and underwrite insurance contracts accordingly.

Increasingly granular risk assessment capabilities will help insurers more easily identify the high-risk consumers most likely to make a claim on their insurance policy. Hyper-personalised risk assessments, coupled with increasingly personalised prices in the insurance sector, could in due time leave certain groups of consumers uninsurable or be at risk of no longer being able to afford the premiums charged by insurance firms. This could lead to their financial exclusion.

Evidence is already beginning to emerge. BEUC's Dutch member Consumentenbond, recently reported a significant increase in home insurance premiums (up to 30%) for groups of Dutch consumers, as insurers expanded their reliance on alternative data provided by big data firms. In some cases, there was clear evidence that the big data insurers relied on was false.[117]

As insurers expand their reliance on Big Data and AI, consumers could be at risk of biased and discriminatory outcomes.[118]

Insurers are currently prevented from basing pricing decisions based on certain protected characteristics, such as race and/or gender. However, other types of data could feasibly act as proxies that can be closely correlated with these protected characteristics (e.g. postcodes signalling ethnicity or occupation categories signalling gender).

In the UK, car insurance comparison websites reported higher premiums for consumers with names suggesting that they are from ethnic minorities. As a result, ethnic minorities often significantly overpaid for their car insurance premiums.[119] Likewise, in the US, evidence emerged of consumers in minority neighbourhoods paying higher insurance premiums compared to other neighbourhoods with similar accident rates.[120]

Consumers should be protected from high risks, and insurers should ensure that the AI systems they rely on do not pose unacceptable risks to consumers. AI systems used for the purpose of pricing and underwriting decisions (e.g. to assess the eligibility or set the premium for a consumer's car or life insurance policy) should be listed as a high-risk activity in the AI Regulation.

[117] https://www.consumentenbond.nl/nieuws/2018/premies-woonhuisverzekeringen-stijgen-door-gebruik-big-data

[118] BEUC addressed this topic in a recent paper: https://www.beuc.eu/publications/beuc-x-2020-039_beuc_position_paper_big_data_and_ai_in_insurances.pdf

[119] https://www.bbc.com/news/business-43011882

[120] https://www.propublica.org/article/minority-neighborhoods-higher-car-insurance-premiums-white-areas-same-risk

12.7. AI and trade

A recent study from vzbv[121], BEUC German member, found that current EU trade negotiations might significantly restrict the EU's ability to regulate in the field of AI in the future, particularly with regard to independent assessments and audits. The study finds that trade rules could impede future EU rules on transparency, certification and accountability. Also, potential rules on the non-disclosure of source code currently under discussion in the World Trade Organisation (WTO) would hinder effective transparency provisions within the AI Act.

It is paramount that EU law makers must adopt trade rules that do not prevent future rules on transparency and accountability. Also, potential rules on the non-disclosure of source code currently under discussion in the WTO must not impact an effective transparency, enforcement, monitoring and independent assessments of AI systems under the AI Act.

[121] https://www.vzbv.de/sites/default/files/downloads/2021/01/21/20-01-19_vzbv_source_code_and_ai.pdf

BEUC The European Consumer Organisation

This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).

The content of this publication represents the views of the author only and it is his/her sole responsibility; it cannot be considered to reflect the views of the European Commission and/or the European Innovation Council and SMEs Executive Agency (EISMEA) or any other body of the European Union. The European Commission and the Agency do not accept any responsibility for use that may be made of the information it contains.