A CONSUMER CHECKLIST ON PROTECTING CONSUMERS FROM THE RISKS OF AI

As consumers, we are likely to interact ever more frequently with artificial intelligence systems. In turn, these systems will undoubtedly get more powerful and extend to everything, from driving our cars to setting our insurance premiums.

While people see a huge potential in this technology, they still have low trust in AI. Our survey found that the majority of consumers fear AI will lead to a manipulation of their decisions and further abuse of their personal data. More than half of the survey's respondents also had low trust in the authorities exerting effective control over AI.[1]

If people don't feel they are protected, they will not feel at ease with AI systems and there is also a risk they interact only with big tech companies they already know, rather than small innovators. Trust in AI can only come about if people can rest assured that there are protections in place when something goes wrong. A strong legal framework is necessary to make the EU the world leader of trustworthy AI.

The EU is currently drawing up the world's first piece of legislation on AI – the AI Act. Although it is welcome, the Commission's proposal falls substantially short of what is needed to protect consumers from the risks of AI.

BEUC recommends that EU decision-makers make considerable changes to the Commission proposal before it becomes law so that consumers can trust AI.

1 BROAD PRINCIPLES AND OBLIGATIONS MUST APPLY TO ALL AI

The proposal must have a broader scope than the current focus on 'high-risk AI systems'. It must establish basic principles and obligations such as fairness, accountability and transparency to all AI. The AI Act should require that all AI-powered appliances or products, such as smart meters, connected toys, virtual assistants, or algorithms that organise what people see on social media, have these principles applied to them.

2 HARMFUL AI SYSTEMS: MORE OF THEM SHOULD BE BANNED

The list of AI practices that are banned must be extended and strengthened to better capture consumer-related risks.

Unacceptable practices such as social scoring, which is when an AI system evaluates the trustworthiness of an individual based on their social behaviour or their preferences, emotions, health or intelligence, should be banned when used by private as well as public bodies. Remote biometric identification systems such as facial recognition used by private entities in public places have no place in our society, as they are too intrusive and damaging of our fundamental rights.

Emotion recognition software should, except in very specific circumstances related to health or research purposes, be banned in line with the recommendations of the European Data Protection Supervisor and the European Data Protection Board.

In addition to physical and psychological harm, the list of banned AI practices should include those that manipulate someone in a way that can cause them economic harm. Also, AI practices should be prohibited when they have the effect (instead of the intention) of causing physical, psychological or economic harm.

AI which exploits any type of vulnerabilities, either temporary such as grief or emotional distress, or through digital asymmetry by using personalisation practices or persuasion profiles, must be forbidden.

[1] BEUC survey: 'Artificial Intelligence: what consumers say: Findings and policy recommendations of a multi-country survey on AI' (2020).

3

CONSUMERS NEED STRONGER RIGHTS WHEN SUBJECT TO AI SYSTEMS

Dealing with an AI system can be frustrating and problematic for consumers as they are not able to understand how the system functions or reaches its decision. In cases where an automated decision has a significant impact on consumers, they should have the right to be given a clear explanation about how an AI system affecting them works, and the right to object the decision.

The AI Act must also grant consumers the means to seek justice and redress in case they are harmed. Consumers should have access to complaint mechanisms put in place by the provider of an AI system. They should also have a right to complain to a national authority, and to launch legal action, when an AI system or practice that affects them breaks the law. In this regard, consumer and civil society organisations should be able to represent consumers in exercising their rights or file complaints if an AI system breaks the law.

The AI Act should also include a right to remedies, including receiving compensation for material or non-material damages suffered, and it should be possible for consumers to launch a collective redress action or injunction under the Representative Actions Directive.

4

EFFECTIVE ENFORCEMENT NEEDED TO TACKLE BREACHES OF THE AI ACT

The EU will have to beef up enforcement of the AI Act by public authorities. One way to help national authorities is to create a highly specialised and independent body of technical experts designated by the Commission. Their role would be to assist with the technical aspects of an investigation at national or EU level, and have the competence to issue non-binding opinions about specific cases brought up by the national authorities.

To avoid bottlenecks and ensure that there is enforcement in case of Europe-wide issues, the European Commission must be able to start an evaluation procedure into an AI system if it believes an AI system presents a risk, if no market surveillance authority has yet started an investigation into it, or if an AI system affects consumers in more than one EU country.

If an authority starts an investigation into a suspicious AI system, it must inform their counterparts in other EU states.

5

THE CONFORMITY ASSESSMENT PROCEDURE MUST BE STRENGTHENED: HIGH RISK APPLICATIONS SHOULD GO THOUGH INDEPENDENT 3RD PARTY ASSESSMENT

The Commission's proposal relies too much on self-assessment, meaning AI developers would self-certify their own systems even if they are high-risk. We believe that any high-risk AI should instead go through third-party assessment and all relevant documentation should be notified to the relevant market surveillance authority before being placed on the market and be made publicly available.

Previous scandals like Dieselgate have shown us how important it is to separate conformity assessment procedures from the manufacturers. We must make sure high-risk AI goes through third party, independent assessment.

6

STANDARDS SHOULD NOT BE USED TO DEFINE OR APPLY LEGAL PRINCIPLES OR FUNDAMENTAL RIGHTS

The Commission proposal makes the assumption that if an AI system complies with yet-to-be-drawn-up standards, it will comply with the AI Act and can be placed on the market. But standards should only be used to implement technical aspects and not to interpret legal requirements.

There is an additional concern: today standardisation bodies are heavily dominated by businesses with little participation from civil society, which could lead to a form of regulatory capture.

BEUC The European Consumer Organisation

April 2022

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EISMEA. Neither the European Union nor the granting authority can be held responsible for them.