The Consumer Voice in Europe

BEUC'S RESPONSE TO THE EUROPEAN COMMISSION'S WHITE PAPER ON ARTIFICIAL INTELLIGENCE

Contact: Ernani Cerasaro – 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-2020-049 - 12/06/2020

Why it matters to consumers

Artificial Intelligence (AI) and Algorithmic-based Decision Making (ADM) applications are already shaping consumers' lives. For example, online video platforms use algorithms to personalise users' content and recommendations; banks use them to track suspicious activities and prevent fraud; public authorities make use of AI and ADM to process and answer citizen requests; smart phones integrate virtual personal assistants and social media applications organise the feeds that consumers see in their timeline on the basis of automated analysis of their past behaviour, online activities and interactions. We are still just at the beginning of the digital transformation of our society. While AI may offer many innovative opportunities for consumers, its widespread use brings profound social, legal and economic challenges affecting consumers and the entire society. A strong regulatory framework is necessary to ensure that the use of AI is adequately regulated and controlled. It should facilitate innovation and guarantee that consumers can fully reap the benefits of the digital transformation of our societies but are protected against the risks posed by AI.

Table of Contents

Summary of recommendations

In response to the European Commission's White Paper on Artificial Intelligence, BEUC make the following recommendations to design a regulatory framework for AI and ADM which responds to consumers' needs and expectations:

1. **The definition of 'AI' provided in the White paper should be refined** and aligned with the one agreed by the AI High Level Expert Group (HLEG)[1]. In addition, we recommend the use of terms such as Algorithmic-based Decision Making (ADM), robotics or algorithmic systems, depending on the context and on the technology.
2. **The proposed risk-based approach** for the development of the new legal framework on AI and ADM **should be revised and broadened**:
    - New rules should not only cover applications considered to be "high-risk''. A broader, more inclusive, approach should be envisaged. Legal obligations should gradually increase alongside the identified level of risk, starting from the principle that some basic obligations (e.g. regarding transparency) should be applicable to all AI applications. From there, the greater the potential of algorithmic systems to cause harm, the more stringent the legal requirements.
    - The new rules should apply to algorithmic systems, including AI, machine learning, deep learning, ADM and robotics regardless of the level of risk. The new framework should be applicable where consumers are users of or subject to an algorithmic system, irrespective of the place of establishment of the entities developing and/or deploying the system.
    - The new rules should also encompass provisions on the admissibility and design of algorithmic systems; organisational and technical safeguards; and establish an institutional structure for effective supervision and enforcement.
    - The process which determines the level of risk of an application (in form of an impact assessment) must be trustworthy, verifiable and objectionable. Such impact assessment should take into account the possible risks arising throughout the whole life cycle of the system for both individuals and society at large. Enforcement authorities should be tasked to propose and update valid methodologies for assessing the level of risks and potential harms.
3. When proposing legislation on AI and ADM, the Commission should **adopt a precautionary approach**. We consider this to be essential to ensure that technologies that pose significant harms for individuals and society are not deployed until they are tested and certified. As an ultima ratio measure, it should be possible to ban the use of certain AI or ADM systems. Self-assessment of compliance with the

[1] BEUC is a member of the European Commission's High Level Expert Group on AI. To download the definition: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60651

new rules by operators should be in principle avoided, at least for the application presenting a high level of risk.

4. Consumers should have control of their data when it is used by AI and ADM products and services. In particular, consumers must know how their data is processed through enhanced transparency provisions and should be able to manage the processing through user-friendly interfaces.
5. The Commission should enshrine a set of AI rights for consumers in any future regulation. This set of rights should at least include: right to transparency, explanation, and objection; right to accountability and control; right to fairness; right to non-discrimination; right to safety and security; right to access to justice; right to reliability and robustness.
6. While highlighting the need to protect consumers, the white paper lacks specific initiatives for mitigating the negative consequences of the widespread use of algorithmic systems on consumers' fundamental rights and wellbeing. In particular, we urge the Commission to specifically address in any future regulation the negative effects of businesses' large-scale commercial surveillance of consumers and its potential influence on their online and offline choices and behaviours.
7. AI has the potential to help achieve the green transition but also comes with a big environmental footprint. We urge the European Commission to explore the opportunities offered by AI but also to consider the environmental harms – such as carbon-dioxide emissions and electronic waste – resulting from the data-driven infrastructures needed to power the large-scale deployment of AI and ADM powered products and services. We recommend incentivising the use of greener infrastructures for the development and deployment of these technologies so that they support the achievement of sustainable development, climate neutrality and circular economy goals.
8. Any future regulation should envisage a **coherent and efficient compliance and enforcement system** which:
    - Obliges businesses to ensure built-in control mechanisms for the development and use of ADM systems.
    - Ensures a high level of protection for consumers via a combination of independent ex-ante verification mechanisms and continued ex-post compliance checks by authorities in presence of high-risks applications.
    - Ensures a coherent structure and harmonised procedures for authorities to deal with pan-European/cross-border infringements.
    - Guarantees the active cooperation among the relevant enforcement authorities, as well as between public and private enforcement bodies, including consumer organisations. Ensures that enforcement authorities are equipped with the necessary financial, technical, and human resources, as well as the necessary legal powers, to do their job efficiently.
    - Provides the enforcement authorities with the necessary powers (e.g. right to obtain information, the right to inspect and access) so that they can scrutinise and evaluate these ADM systems and impose penalties in case of law infringements.

- Ensures that companies are transparent about their use and expected results of ADM systems and processes and build in specific interfaces in order to allow authorities to exercise meaningful oversight and ultimately enforce the rules (**compliance by design**).
- Ensures the availability of effective remedies for consumers and the accessibility of procedures to claim the violations of their rights through the use of ADM systems and AI technologies.

9. An **updated liability framework for digital goods and services is urgently needed** to ensure effective access to justice for consumers when things go wrong with their products. In particular, we call for a sound revision of the Product Liability Directive[2].
10. An **updated legal framework on consumer protection**, including **safety legislation**, is equally needed to ensure that consumers are fully protected against the risks created by AI products and services. In particular, we urge the Commission to modernise the General Product Safety Directive (GPSD).

[2] For more info on our position on product liability, please refer to our recent position paper "Product Liability 2.0: EU rules fit for consumers in the digital age", published in May 2020.

Introduction

On 19 February 2020, the European Commission published a 'White Paper on Artificial Intelligence: A European approach to excellence and trust'. The aim of the Commission is to launch a European strategy promoting the uptake of AI and addressing the risks associated with certain AI applications. Europe's ambition is to become a '*global leader in innovation in the data economy and its applications*' by fostering a development of an AI ecosystem which profits citizens, business and public sector. The White Paper identifies two main elements allowing for such an ecosystem to arise: excellence and trust.

For the creation of an 'ecosystem of excellence', the Commission focuses on concrete actions to support research, development and uptake of AI across the EU economy and public administration. For the creation of an 'ecosystem of trust', the Commission builds on the AI High Level Expert Group "Ethics Guidelines for Trustworthy Artificial Intelligence", published in April 2019. These guidelines identify seven key requirements for the development of trustworthy AI applications: human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal and environmental wellbeing; accountability.

The Guidelines, however, are not legally binding. In light of this, and in line with the Commission President's political guidelines, the White Paper recognises the need for a European regulatory framework which would build trust among consumers and businesses, and therefore speed up the uptake of the concerned technologies.

The Commission's White Paper sets out a first outline of a possible new regulatory framework which is based on a risk-based approach. BEUC agrees that a risk-based approach is appropriate. However, we are concerned that an approach which, as envisaged by the Commission, focuses solely on high risk applications would significantly reduce the scope of the new rules and ultimately inadequately protect consumers.

While AI applications are already subject to European legislation *inter alia* on data protection, privacy, non-discrimination, consumer protection, product safety and liability, the existing regulatory framework is not fit for purpose to address the risks posed by AI. Therefore additional measures are needed[3]. Consumers expect effective protection and respect of their rights whether or not a product or service relies on AI.

Recent developments following the COVID19 pandemic have brought AI to the spotlight once again, highlighting its potential to improve health treatments for example. While we recognise that AI has a lot of positive potential, we would like to highlight that the current situation does not change the fact that AI comes with many challenges and risks which require the use of this technology to be properly regulated.

[3] We already expressed some of our concerns in other position papers: AI rights for consumers; Automated decision making and Artificial Intelligence; AI must be smart about our health; Access to consumers' data in the digital economy; When innovation means progress - BEUC's view on innovation in the EU.

1. PROBLEM DEFINITION: WHAT IS AI?

Before addressing the practical and regulatory implications of AI, we must agree on its definition.

As a starting point, it is worth highlighting that there is no common nor legal definition of AI, and that the definition provided by the Commission in its White Paper should be considered overly simplistic. For the sake of straightforwardness, we often refer to "AI systems", "AI applications", "uses of AI", and similar. The concept of AI is blurry and can embrace different perspectives. The reason is quite simple: there are thousands of different techniques currently used to develop very complex and (partially) autonomous technologies that can fall into the artificial intelligence basket. At a regulatory level there are different definitions of AI being used[4]. In the European regulatory framework, a first definition was provided in the "Ethics guidelines for trustworthy AI", published by the European Commission AI High-Level Expert Group[5] (AI HLEG) in April 2019[6]. Based on this definition, AI can be either a system (software or possibly hardware) or a scientific discipline. In the first case, such a system should have:

- a human mind that designs the technology;
- a given dataset (structured or unstructured);
- a complex goal to be achieved autonomously;
- a reasoning on the knowledge acquired from the dataset;
- a scientific technique to be applied;
- the capability to behave;
- the capability to adapt to external reaction on its previous actions.

However, in an attempt – albeit understandable – to provide a simple and straightforward definition, in its White Paper, the Commission states that: *'Simply put, AI is a collection of technologies that combine data, algorithms and computing power'*. As is evident from the abovementioned definition adopted by the AI HLEG, this wording cannot be considered sufficient to define AI and the Commission should take utmost account of this.

The White Paper's definition, in fact, could almost be applied to any software ever written. This definition lacks crucial components of what AI is. By only referring to data and algorithms in combination with computing power it does not explain the behavioural characteristics of AI and it overlooks the social and human context where AI technology is created[7]. It does not explain its purpose: Is AI modelling human behaviours? Is it modelling human thoughts? Is it a model that can behave intelligently? Is it a mix of all of this?

Having a solid definition is crucial and has major regulatory consequences. If we were to follow the definition provided in the White Paper at regulatory level, all the concepts that descend from it could be questioned by simply arguing that a specific application cannot be considered as AI. Such a definition would allow organisations to easily bypass and circumvent future regulations and would ultimately lead to lack of accountability.

[4] See, for example, US FUTURE of Artificial Intelligence Act of 2017.
[5] To download the definition: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60651
[6] A first draft of the Guidelines – then subject to public consultation - was published in December 2018: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai
[7] Yoshua Bengio, one of the godfathers of AI, defined it as: *"[AI is] about making computers that can help us that can do the things that humans can do but our current computers can't."* Although it is not adaptable to a regulatory instrument, this definition allows us to understand why and how AI was born and developed.

Then, if we want to use AI as a term, it is first of all appropriate to debate on a valid and comprehensive definition which could encompass present and future applications creating risks for individuals (persons or legal entities), for society at large and for specific social groups. For the time being, our proposal is to use more specific terms depending on the context, not reducing everything to AI. Thus, it seems that the use of algorithmic based decision making (ADM hereinafter) is more aligned with the regulatory objectives HLEG of the white paper and more suitable to define its action field.

ADM is a technology neutral term, that includes the technologies that the AI HLEG and the public generally referred to as artificial intelligence. In the same line, the German data ethics commission chose to focus on 'algorithmic systems', rather than 'artificial intelligence'. An ADM system comprises much more than just program code or an algorithm. It refers to the entire process from data acquisition and data analysis to the interpretation of the results and the derivation of a decision or recommendation from the results[8]. ADM systems are characterised by the fact that they contain an algorithmic component (control system) which produces an output (decision) on the basis of an input and outputs it in the form of a (numerical) value. As such ADM-Systems also include 'learning' systems that derive decision rules from data by means of machine learning and can adapt them over time. The systems discussed under the keyword artificial intelligence (AI) usually fall under this definition. The key element of the term 'ADM-System' is its relevance from a policy point of view, as it stresses the element that the system produces an output that is used to prepare or make a decision that has an impact on people or legal entities.

2. A REGULATORY FRAMEWORK FOR AI AND ADM

2.1. The scope of the EC proposal and its risk-based approach

Consumers' concerns in relation to AI and ADM systems range from the lack of transparency, to concerns about safety, unintended consequences and malicious uses. For example, as shown in a survey commissioned by our German member Verbraucherzentrale Bundesverband (vzbv) automated decisions are regarded as a risk for 75% of consumers if the underlying data and principles applied are unclear[9]. The new regulatory framework for AI and ADM must properly address the whole set of consumer concerns and ensure that this technology is developed and deployed in a manner that embeds strong and tangible safeguards during its whole lifecycle. Such safeguards should be ensured to anyone who is affected by an ADM system.

To ensure a trustworthy development of AI technologies, the White Paper refers to the non-legally binding requirements stipulated by the Ethical Guidelines of the AI HLEG: human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal and environmental wellbeing; accountability.

Although these points certainly contribute to shape more trustworthy technologies, these guidelines are not legally binding. To date, there is no specific legal framework at EU level aimed at regulating AI. That being said, AI applications are in certain instances already subject to a range of existing laws (e.g. data protection and consumer protection legislation), as it happens with any other products or services falling into the scope of such laws. For example,

[8] Vieth, Kilian; Wagner, Ben: Teilhabe, ausgerechnet (2017), URL: https://www.bertelsmann-stiftung.de/de/publikationen/publikation/did/teilhabe-ausgerechnet [16.04.2019].
[9] https://www.vzbv.de/sites/default/files/2019_vzbv_factsheet_artificial_intelligence.pdf

if the use of a chatbot for customer support in the EU is processing personal data for delivering solutions to the consumer (which means that it needs process the customer's information, communications, etc.), such a technology should respect the General Data Protection Regulation (GDPR).

In its White Paper, the European Commission acknowledges that existing legislation may not be effective or might otherwise be difficult to apply in the case of AI technologies. This principally because of the inner opaqueness of such technologies (so-called "black box-effect"), their complexity, volatility and autonomy.

The White Paper therefore sets out the possibility to adapt existing legislation and add new rules. BEUC welcomes that the European Commission wishes to examine how to adapt existing legislation – such as EU legislation on product safety and product liability – to ensure an effective consumer protection and re-think the allocation of responsibilities between those actors involved in the development and deployment of technologies (developers, business, etc). As BEUC has repeatedly highlighted the need to update the EU's current rules and bring them up to speed with technological developments. The Commission also identifies a potential need for additional regulation to address the risks inherent to the use of AI. For the purpose of designing these new rules and obligations, the Commission puts forward a risk-based approach.

BEUC considers that new legislation is necessary to address the risks posed by AI and ADM and also that such legislation should adopt a risk-based approach. In this sense, we welcome the direction envisaged by the Commission. We are however concerned about the risk assessment methodology, the risk management and the narrow scope of the new legal regime envisaged by the Commission, as explained further below. In particular, we underline that the mere fact that certain applications pose a higher risk than others, doesn't mean that only such riskier applications should be further regulated.

The main risks identified by the Commission are related to fundamental rights (in particular, data protection and non-discriminations) and to safety and the effective functioning of the EU liability regime (e.g. safety risks related to autonomous vehicles and allocating liability if such car causes an accident). On the basis of these main risks, the White Paper draws a clear-cut line between high-risk AI applications and all other AI applications. The new legal obligations envisaged by the Commission would only apply to high-risk applications. Such applications would face stricter legal requirements, including for example technological conformity assessments and, in some cases, mandatory regulatory pre-approval before market deployment. AI applications not considered high risk would be exempted from these new legal requirements, the only additional measure envisaged for such applications would be a voluntary labelling scheme awarding those which meet certain EU-wide, yet undefined, standards. According to the White Paper, for an AI application to be classified as high-risk two **cumulative** elements should be present:

1) **High-risk sector**: the technology is developed in a sector where "*significant risks can be expected*". Such high-risk sectors should be "*specifically and exhaustively*" individuated by the new legislation and might initially include "*healthcare; transport; energy and parts of the public sector*." Such a list should be "*periodically reviewed and amended where necessary*." In addition to these sector-based high-risk applications, the Commission expects "*exceptional instances [where] … the use of AI applications for certain purposes is to be considered as high-risk as such[.]*" as "*the use of AI applications for recruitment processes as well as in situations impacting*

workers' rights, … specific applications affecting consumer rights" and facial recognition technology.

2) **High-risk use**: high-risk sector technologies are "*used in such a manner that significant risks are likely to arise*". Such uses include "*uses of AI applications that produce legal or similarly significant effects for the rights of an individual or a company; that pose risk of injury, death or significant material or immaterial damage; that produce effects that cannot reasonably be avoided by individuals or legal entities*".

According to the White Paper a sum of the two abovementioned conditions would ensure a narrow scope of application while, at the same time, providing the maximum level of legal certainty.

Although BEUC share's the view that new additional regulation is necessary, we think that the risk-based approach envisaged by the Commission is too narrow in scope and lacks nuance:

- First, the definition of high-risk provided in the paper is tautological. To define whether there is a high-risk, the elements to be taken into account are still high-risks which remain undefined. We encourage the Commission to redefine such a concept, specifying and elaborating on the concrete and precise factors that would cause risks for individuals and society. In this sense, we would recommend to follow the example of the opinion of the German Data Ethics Commission, according to which a risk-based approach addresses AI applications "*which are associated with regular or significant potential for harm*".
- Secondly, **regulating by sectors is confusing and unsuitable**. While we acknowledge that some AI applications present higher risks than others, if the binary approach put forward in the White Paper is accepted, we believe that the scope of the regulation is too narrow render any future measures ineffective. It would, in fact, contradict the obligation to provide for a high level of protection for consumers across all sectors. In our opinion, first there is a need for a **horizontal intervention that covers all sectors** and which possibly takes into account the single specificities of a given sector. When introduced as a cumulative requirement, the ex-ante identification of high-risk sectors could cause a dangerous illusion for consumers subject to technologies classified as 'not risky'. For example, AI tools present in everyday consumers' lives such as smart cars, home assistants, drones for delivering, algorithmic selection of social media feeds, music and media streaming would fall outside the scope but also financial services. Although it is true that all these services may present a different level of risk, it is equally true that it is not possible to exclude that they will fit into a low or high risk category only because they are part of a given sector. Furthermore, technologies often do not differ from each other as per sector. We wonder why a certain decision in sector X, adopted on the same parameters and with the same techniques as a decision adopted in sector Y, must be assessed differently if the damage is caused by a biased or inaccurate algorithm.
- Lastly, a bifurcation of AI into high and low/no risk as envisaged by the Commission fails to capture the essence of the risks in AI technologies. The starting point should be that **AI deployments can be risky as such** but, as they have different intensities, can be mitigated.

A careful analysis of the actual digital world demonstrates that the deployment of AI technology should be approached cautiously, keeping in mind the real and present dangers

brought by this technology[10]. Generally speaking, **over-stating the potential benefits of AI or having a too narrow approach towards its risks can have very negative consequences**. The Commission itself states that AI can generate harm and that such harm can be material (safety and health of individuals, including loss of life, damage to property) and immaterial (loss of privacy, limitations to the right of freedom of expression, human dignity, discrimination for instance in access to employment). We should not lose sight of all these risks and ensure regulation brings a high level of protection against them.

2.2. Specific requirements for high-risk applications

The distinction between high-risk and non-high-risk applications envisaged by the Commission has consequences in terms of legal requirements which would be applicable, depending on which category the application in question falls into. Only high-risk AI solutions would be subject to specific requirements in relation to training data, keeping records of data, transparency requirements, robustness & accuracy, human oversight. In addition, the Commission suggests a prior conformity assessment, possibly including procedures for testing and inspection of certification of algorithms and data sets.

BEUC welcomes the provision of such requirements which are certainly capable of contributing to a more transparent and responsible development of new technologies.

While waiting for these requirements to be better specified by the Commission in a clearer regulatory framework, we underline that, we need a gradual approach to risk assessment and corresponding mandatory requirements for each risk-level. These requirements, **should thus not be limited to high risk applications**. Even more so if the risk is identified through inaccurate or unclear factors.

3. THE WAY FORWARD

The future EU law on AI is a crucial test for Europe's digital policy. Europe must design a regulatory framework that ensures that innovation can flourish in a way that is respectful of individuals' fundamental and consumer rights and of our societal values. The Commission must ensure it captures and properly considers all the various aspects relating to the sustainable development and deployment of powerful and intelligent technologies in our markets and society.

The narrative throughout the White Paper indicates that the Commission is aware of the challenges we are facing and takes them seriously. The two building blocks of the White Paper, an 'ecosystem of excellence' and an 'ecosystem of trust,' are well-grounded. However, there are several elements where greater nuance and a more concrete approach would be required.

One of the shortcomings of the White Paper is that while consumers are mentioned in different parts, there is no focus on the specific risks arising for them when using AI and ADM technologies. Algorithmic advanced systems might cause adverse impacts for consumers which are not properly addressed in the White Paper, such as discrimination or social and economic exclusion. For example, in the case of big data analytics algorithms are used to create credit scores and inform loan screening also via the incorporation of non-financial data

[10] For example, the U.S. National Institute of Standards and Technology recognises biases in AI facial recognition tools. Recently, a Dutch court stated that bias in systems to detect welfare fraud determined a violate human rights. Racial bias in a health care delivery algorithm was discovered by researchers after the algorithm being used for years. Alike, unfortunately, many other examples could be quoted.

sets (such as where people live, internet browsing habits and purchasing decisions). The decisions taken on the basis of the algorithmic reasoning of these systems are largely unregulated while they are often discriminatory. However, the White Paper does not seem to consider them in its regulatory proposal. Similarly, while the intention behind the human-centric approach of the Commission seems well-defined, there is a lack of critical socio-political analysis surrounding diversity, equality and environment which constitute indispensable aspects for such humanistic development to take place.

Finally, we underline the importance of building a regulatory spectrum that enables a fairer access to technology. Such belief is the building block for ensuring that the interests of marginalised and vulnerable consumers are adequately taken into account. In this sense, we would encourage the Commission to introduce a duty of care for developers in order to deploy consumer-oriented systems. In particular, by incentivising a consumer-centric approach we could safeguard access to all intended users avoiding exclusions especially for those consumers who are currently left behind.

In the following sections we describe some of the main elements where we expect the Commission to develop a more detailed and ambitious approach.

3.1. A precautionary approach and more gradual establishment of risks and corresponding legal requiremements

One of the major weakness of the Commission's White Paper is the absence of a precautionary approach to the development and use of AI and ADM systems. It would seem that the intention of the Commission is to allow the development and use of the ADM services/products regardless of their riskiness. For example, the word 'ban' is never mentioned in the White Paper except when referring to the work done by the German Data Ethics Commission.

We consider it is essential that the assessments with regards to the risks for individuals and society are developed in the form of a **preventive impact assessment**, as to allow the **blocking of highly dangerous technologies**.

- The causes of risk must be assessed from the conceptual phase of the system and must, to the fullest extent possible and according to the state of the art knowledge, foresee possible harms during its whole lifecycle. Furthermore, the **risks should be considered as a non-exhaustive list** and should take into account numerous factors, including: the type and nature of the data used (e.g. personal/non personal data); the type of algorithmic model; the types of logical reasoning carried out by the system; the security measures put in place; the methods used to test and maintain the system; sectors; harms for the environment; the desirable dissemination of the product/service; the business model.
- The process which determines the level of risk of an application (in a form of a preventive impact assessment) must be trustworthy, verifiable and objectionable. Such **preventive impact assessment** should take into account the possible harms arising throughout the whole life cycle of the system for both individuals and society.
- **Authorities should be tasked to develop a methodology and to set the criteria needed to define the level of risk** of an application. The authorities could refine this set of criteria and the methodology depending on different sectors.
- The intensity of the risk can go from a **low level up to irreversible harm for the individual or the society**, in which case the technology should be banned. For example, some companies are investing more and more resources into very intrusive and potentially very harmful technologies such as those meant to figure out how to objectively "read" emotions in people by detecting facial expressions. However,

researchers demonstrated that "*the science of emotion is ill-equipped to support any of these initiatives.*[11]" For this reason we think that businesses intending to use such form of emotion recognition should not have access to markets (as already happens) until it is demonstrated that such practices are not harmful and can fulfil the respective risk mitigating requirements.
- Legal obligations should gradually increase alongside the identified level of potential harm, as described in the German data ethics commission opinion.

3.2. Approach to data management and control must favour consumers and public interest

Data is a crucial resource of the digital economy and it can be indispensable for the development of services and products powered by algorithmic technologies. A future regulatory framework for algorithmic systems should take outmost account of various aspects relating to data and ensure a consumer centric approach to data access and control.

- Consideration should be given to **power asymmetries** between institutions, businesses and individuals arising from the growth of digital devices and systems and the rapid expansion of digital data that they generate. Where appropriate, for instance in situations of individual or collective harm, consideration should be given to whether additional regulatory measures to those stipulated by the GDPR may be needed to address this (please, also refer to point 3.4 below).
- Second, it is important to ensure that consumers are fully aware of what happens with their personal data, as also required by the GDPR. Consumers should always be **informed** in a timely clear and intelligible manner about the existence, process and rationale of algorithmic systems.
- Third, consumers should be fully in **control** of their personal data. While it is important to ensure competition among businesses also by allowing them to access essential data, personal data sharing always has to be done under full control by consumers and in compliance with the GDPR's right, obligations and principles.

3.3. AI must not further entrench digital commercial surveillance

The development of algorithmic technologies is directly linked to the widespread growth of 'intelligent' services and products on the market. Such technologies are rapidly changing the way that consumers search and shop for products. For example, a current trend is the use of devices such as smart assistants allowing consumers to search and order products using voice commands (e.g., Amazon's Alexa).

While these new AI powered products and services may have many attractive features and could provide benefits like customised services, they also provide the possibility to monitor and analyse consumers' behaviour in detail and therefore to greatly influence their choices. AI and ADM technology elevates the levels of pervasiveness and power of the so-called commercial surveillance ecosystem that has come to dominate the online world, further endangering consumer's autonomy and freedom of choice.

Digital services rely on algorithm powered technologies for processing consumer data and for targeting consumers with ads and other messages. Algorithms can be used to exploit

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

consumer's weaknesses and biases in order to convince them to purchase products limiting their choices. Via massive data collection, companies are able to oversee consumers' online activity, record it and use it to discover possible correlations that may be useful in influencing consumers through the most effective ads[12].

The wide diffusion of smart products and services is also able to incentivise price discriminations among consumers. It has been demonstrated that it is efficient for a brand operating in a competitive environment to price discriminate less tech-friendly consumers across distribution channels[13]. Consumers with clearer preferences find discounts and reduced prices that are often unavailable to those who are less customary to using online marketplaces. In this sense, we highlight that there should be no price differentiation by means of personalised and non-personalised automated assessments. Moreover, it is important to bear in mind that services are often provided 'for free' in order to maximise the number of users and therefore the amounts of profit-generating consumer data collected for AI and ADM systems. The scope, invasiveness and potential consequences of this commercial surveillance is difficult, if not impossible, for consumers to comprehend. This happens, for example, in the context of digital advertising or social networks.

In our opinion, in presence of such phenomena, the potential damage suffered by the individual consumer or by a group of consumers can be very high. However, the Commission White Paper seems not to embrace "everyday" activities such as shopping activities within its definition of high risks.

We therefore call on the Commission to restrict the use of systems building on consumers' commercial surveillance and to encourage the deployment of consumer-centric systems based fair and non-discriminatory practices.

3.4. Consumers must have a strong set of rights

In our 2019 position paper[14] "AI rights for consumers", we outlined a non-exhaustive list of AI rights ensuring a fair, safe, and just society and set to guarantee a high level of consumer protection. We urge the Commission to concretise these rights in its future legislative proposal by translating them into enforceable rules so that ADM powered technologies serve consumers and does not harm them. In particular, at least the following rights should be guaranteed:

Right to transparency, explanation, and objection: consumers should have a right to get a clear picture of how decisions that affect them are made and be able to oppose wrong or unfair decisions and request human intervention. In particular consumers should be able to object automated decisions independently of the restrictions individuated by article 22 GDPR, i.e. that such decisions are taken 'solely' on automated data processing, that the data processed is qualified as 'personal data', and that such decisions should have 'legal effects' or 'similarly significantly affect' them. We have concerns that if such right to object is aligned to the GDPR article 22 as far as its scope is concerned, commonly used automated decision-making processes that have an impact on consumers would not be able to be objected.

Right to accountability and control: consumers should have a right that appropriate technical and organisational systems as well as measures are put in place that ensure legal compliance and regulatory oversight.

[12] Sartor, G., New aspects and challenges in consumer protection, Study for the committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2020.
[13] Liu, Yi & Yildirim, Pinar & Zhang, Z. (2019). Artificial Intelligence and Price Discrimination.
[14] https://www.beuc.eu/publications/beuc-x-2019-063_ai_rights_for_consumers.pdf.

Right to fairness: consumers should have a right that algorithmic decision making is done in a fair and responsible way.

Right to non-discrimination: consumers should have a right to be protected from illegal discrimination and unfair differentiation.

Right to safety and security: consumers should have a right that ADM-powered products are safe and secure throughout their lifecycle.

Right to access to justice: consumers should have a right to redress and public enforcement if risks associated with ADM materialise.

Right to reliability and robustness: consumers should have a right that ADM-powered products are technically reliable and robust by design.

3.5. A strong and streamlined approach to sustainability and environmental protection is needed

Digitalisation and AI can help the urgently needed green transformation and the move towards more global sustainability. But it 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 ADM and AI. Empirical findings have shown that digital technologies contribute to 4% of overall greenhouse gas emissions, a number expected to double by 2025[15]. Other studies show that training a single AI model emits carbon dioxide in amounts comparable to that of five cars over their lifetimes[16]. This problem must not be underestimated, particularly in the context of the European Green Deal. In this sense, a general rethink of political strategies is needed 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 safeguards. The Commission must provide more clarity how it intends to ensure that generalised development and extended access to algorithmic technologies is carried out in compliance with environmental requirements.

In particular it is key to ensure that the development of innovative technological solutions will address sustainability challenges, by for example incentivising companies to reduce the carbon footprint of data centres and IT devices (including smartphones). While certain measures have already been taken such as addressing the energy efficiency of servers through Ecodesign measures and by proposing a new strategy on ICT products as part of the second Circular Economy Action Plan, much more needs to be done in relation to the scale of the problem. Besides handling the infrastructure which underpins the internet and AI in a sustainable manner it will be crucial to shape digitalisation in a way that it can serve a fundamental transition towards sustainability.

[15] Maxime Efoui-Hess, *Climate Crisis: The Unsustainable Use of Online Video*, Shift Project (2019)
[16] Karen Hao, Training a Single AI Model Can Emit as Much Carbon as Five Cars in Their Lifetimes, MIT Tech. Rev., https://www.technologyreview.com/s/613630/training-a-single-ai-model-can-emit-as-much-carbon-as-five-cars-in-their-lifetimes/ ; Emma Strubell, Ananya Ganesh & Andrew McCallum, Energy and Policy Considerations for Deep Learning in NLP, Ann. Meeting Ass'n Computational Linguistics (2019).

3.6. Liability rules must be updated to ensure compensation in case of harm arising out from AI-powered products

As the Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics[17] (hereafter "the Report") accompanying the AI White Paper highlights, AI and ADM technologies nowadays **importantly disrupt liability rules[18]**. In parallel, EU and national liability rules have been designed with traditional business models and traditional products in mind. For example, products that the drafters of the Product Liability Directive had in mind in the 1980s are a far cry of those surrounding consumers nowadays. The existing framework established by the Product Liability Directive in 1985 is no longer adapted to the multiple challenges brought by new technologies in 2020. This situation creates legal uncertainty for both businesses and consumers, multiplies risks of unequal treatment of consumers in the Single Market, prevents redress and ultimately hinders trust in digital goods in general. An **updated liability framework for digital goods is urgently needed** to ensure effective access to justice for consumers when things go wrong with their products.[19]

We therefore call on the Commission to take outmost account of the following recommendations:

- Liability rules for digital goods should ensure a **higher level of protection** for consumers and should be **fair and cost-effective**.
- In order to mitigate the existing informational asymmetries, we notably call for a **reversal of the burden of proof**: it should be up to the party that has access to the relevant information to investigate the cause of the problem when problems arise.
- The liability framework should be **clear and enforceable.** The fact that multiple actors may potentially intervene in the product supply chain (e.g. manufacturer, app developer, programmer, designer, etc.) should not prevent consumers from obtaining compensation. All professionals involved in the supply of digital goods should be held jointly liable in case of harm.
- Liability rules should provide **the right set of incentives** to all actors involved in the supply chain. Actors should be required to fully internalise the risks of their products and to take the precautionary measures that would prevent harmful situations from occurring in the first place.
- Among others, the notion of "product", "defect", "producer" and "damage" should be revised and adapted to the digital context.
- Targeted changes in national liability based on a **risk-approach** rules should be carefully assessed. In any event, **these targeted changes should by no means replace a sound revision of the Product Liability Directive**.
- Finally, if special liability rules were to be introduced for some categories of digital products, it will be essential to clarify the interplay between the upgraded EU product liability framework and the special liability rules applying for certain AI products. Again,

[17] European Commission, COM(2020)64 final.

[18] This situation precludes consumers from obtaining compensation when things go wrong. Digital goods relying on algorithms are overly complex, opaque, data-driven, may evolve in directions that were not initially expected and vulnerable to cyberattacks. For example, in February 2020, a research conducted by the Dutch consumer organisation Consumentenbond revealed that many 'smart' products are vulnerable to hacks. Consumentenbond tested 10 products and found security issues with two sex toys, two children's GPS watches and two baby cameras. In total, the investigations and hack tests revealed 27 vulnerabilities: www.consumentenbond.nl/nieuws/2020/fabrikanten-laks-met-veiligheid-slimme-apparaten

[19] In May 2019, the European Parliament already regretted "that no legislative proposal was put forward during [the last] legislature, thereby delaying the update of the liability rules at EU level and threatening the legal certainty across the EU in this area for both traders and consumers" (European Parliament, P8_TA(2019)0081, 12 February 2019, pt 132).

such a consistency and coherence are necessary for ensuring a clear and enforceable liability framework for all stakeholders.

We have further detailed the necessary changes in our recent position paper "Product Liability 2.0: EU rules fit for consumers in the digital age" published in May 2020.

3.7. Existing legislation must be updated to ensure consumers are adequately protected

In addition to liability rules, also safety and consumers' rights legislations need to be updated.

In particular, in our forthcoming position paper "Views for a modern regulatory framework on products safety" we call for a **modernisation of the General Product Safety Directive (GPSD)** adopted in 2001. Although the Directive constitutes a key piece of consumer protection policy especially by creating a general obligation for producers to place only safe products on the market, it is now outdated and unable to grasp the challenges arising from technological developments such as AI and ADM technologies. For example, the current legal definition of "product" does not explicitly include software that may be incorporated in a connected product or downloaded after its placing on the market. In this sense, we are concerned that if a safety issue arises due to a software update or inefficiency consumers would not be able to be sufficiently protected. Similarly, the current definition does not offer clarity about who is responsible for the safety of self-learning AI products. We have therefore issued some recommendations for an update of the rules. Among others, we underline the need to establish a principle of "security by design and by default" which constitutes a priority for connected products. This would for instance require manufacturers of such products to respect minimum cybersecurity requirements (e.g. strong authentication features; encryption) from an early stage of and throughout their design process, before putting their products on the market.

Regarding the EU consumer law aquis, it is necessary to assess whether horizontal legislation regarding unfair commercial practices, unfair contract terms, and consumer rights when buying on-line (just to name a few central pieces of consumer protection legislation) are still fit for purpose. For example, as outlined in a previous position paper the law on unfair commercial practices has its roots in the idea that consumers must be given essential information so that they can make an informed decision. Is "essential information" still a valid concept when nobody can retrace why and how a specific decision has been taken?

A targeted REFIT exercise should be undertaken to evaluate whether these directives can still effectively meet their legislative objectives in an ADM environment.

3.8. A coherent oversight, enforcement and redress system is necessary

In order to ensure the trustworthy deployment of algorithmic based technologies, the Commission recognises the need for the applicable legal requirements to be complied in practice and be effectively enforced both by competent national and European authorities and affected parties at national and European level. The Commission also underlines that competent authorities should be in a position to investigate individual cases, but also to assess the impact on society.

The proper functioning of any future regulation will depend on the effectiveness of its provisions and therefore on strong, clear and sound public enforcement. But it will also depend on providing the necessary means to civil society, and in particular consumer organisations,

to fulfil their role as market watchdogs, either via testing of products and services, private enforcement, such as collective redress actions, or via the collaboration with public authorities by providing them with alerts about illegal practices or market failures.

For this to happen, it is firstly crucial to disclose information about each automated decision system, including details about its purpose, design features, potential use and implementation timeline in order to ensure that ADM systems are comprehensible for consumers and supervisory authorities. This way, consumers' trust will increase and authorities will be able to scrutinise systems and consequently minimise the harms by imposing modifications, restricting or prohibiting the use of the system.
Strong oversight by supervisory authorities should be ensured regardless of the level of risks. We also highlight the need for closer cooperation among the authorities, and for an enforcement system that can deliver EU wide results for EU wide infringements/challenges, ensuring a harmonised and effective approach.

Our recommendations can be summarised as follows:

3.8.1. Control and oversight

- ADM technologies should as a matter of principle be subject to **independent control and oversight**. Whether an algorithm-based decision is accurate, fair, or discriminative can only be assessed if an appropriate control system is in place. As a general principle, companies and operators should be able to demonstrate that they comply with the law, such as rules on consumer or data protection, as well as non-discrimination rules.
- In the **pre-marketing phase**, at least for high risk applications, it should be mandatory for a producer/service provider to involve independent third-parties which assess legal compliance and can for example request design changes before a product goes into mass production or a service can be brought to the market.
- For applications that present the highest levels of risk, **ex-ante scrutiny procedures by authorities** (e.g. regulatory pre-approval before market deployment, publication of impact assessments) should be put in place.
- For the **post-marketing phase**, it will be important to ensure that the compliance of a certain product or service with the legal requirements of any future regulation will be assessed during its whole lifecycle, establishing a principle of '**continued conformity'**. This concept is particularly important in an advanced technological environment as recurring software updates and self-learning algorithms may change the properties of products and services over the time and consequently have an impact on how the system respects the legal requirements. Therefore, continuous internal and external control and oversight will be crucial to keep consumers protected.

3.8.2. Accountability and transparency

- Depending on the level of risk, **accountability measures** should comprise ADM impact assessments, documentation, internal audits or transparency measures for the users.
- **Operators must be transparent about their business model and use interfaces** which will allow authorities to exercise meaningful oversight and ultimately enforce the rules.
- To enable both ex-ante and ex-post assessments, independent third-party testing and enforcement measures by Member States, companies need to be accountable and must put in place measures to allow for external control of their ADM systems.
- Rules for an effective auditing system should be put in place so that authorities are able to check the compliance of relevant ADM processes. This would also reveal which —

potentially unintended — consequences the processes have for consumers' everyday lives[20].

- The Commission should also evaluate the possibility of imposing the use of mandatory standards for technical design, logging, documentation and description of ADM systems (**transparency by design**)[21].

3.8.3. Enforcement

- Enforcement authorities should have the necessary powers (e.g. right to obtain information, the right to inspect and access) so that they can **scrutinise and evaluate AI and ADM systems and, in case of law infringements, stop illegal practices, impose remedies and award damages where relevant as well as impose penalties.**
- Authorities must also be capable of conducting **ex post checks** on relevant ADM systems at any time. It must be possible, in particular for the competent supervisory authority, to review and verify the tests performed by the operators.
- .

3.8.4. Remedies

- We also recall the importance of ensuring that **effective remedies** for consumers are easily available. Consumers should have the concrete possibility to interact with a human able to handle and explain the processing activities of the system and its decisions. It should be guaranteed a minimum level of human oversights so that the system's decisions can be checked, timely contested and corrected.

4. VOLUNTARY LABELLING SYSTEM AND LOW-RISK APPLICATIONS

The Commission envisages the possibility of introducing a voluntary labelling scheme for those applications that would not fall under the high-risk category and therefore into the scope of the new regulation. In our view, such a scheme is not suitable to provide meaningful protection to consumers, even if it is just envisaged for low-risk applications.

Labels are fruitful only in relation to the requirements and enforcement systems they are based on. Once clear legal rules and enforcement mechanisms will be in place, the role of a trustworthy label could be considered. It is important to also bear in mind that the inherent information asymmetry in complex and evolving algorithmic learning systems, makes the role of a label very complex and different from other sectors such as environmental, fair trade or food labels for products and services which do not change properties constantly.

5. BIOMETRIC TECHNOLOGIES

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

[20] See BEUC's German member (vzbv) factsheets 'ARTIFICIAL INTELLIGENCE: TRUST IS GOOD, CONTROL IS BETTER'.
[21] REGULATION OF ALGORITHMIC DECISION MAKING FOR THE BENEFIT OF CONSUMERS – by BEUC's German member (vzbv).

smart phones or to authenticate/identify customers in the context of financial services. Retailers can leverage facial recognition to identify a premium customer. Biometrics are particularly sensitive data, and their illegitimate processing can have very serious consequences. For example, one aspect which is very worrying for consumers is the use of biometrics for emotion recognition (e.g. real time facial recognition that analyses feelings and adapts what consumers see/or are offered accordingly). This can lead to serious infringements of consumers' privacy as well as to their manipulation. Due to their inner intrusiveness, the White Paper assigns to the use of biometrics a specific role in the regulatory landscape, considering the need to provide with 'specific requirements' for their use.

The White Paper rightly distinguishes biometric data processed for the purpose of customer authentication, from those used to identify them. This second category[22] certainly raises more concerns than the first (which is however not harmless) and pose greater risks of harm.

Biometric identification systems are already covered by the General Data Protection Regulation (GDPR). The processing of biometrics data for uniquely identifying purposes, such as facial recognition, is forbidden pursuant to Article 9(1) of GDPR, unless it falls under the scope of one of the exemptions listed in such article. Thus, an effective implementation of GDPR may ensure that facial recognition is used in a duly justified manner and does not excessively interfere with the right to privacy. However, when these systems are used – especially in public spaces – ethical and social questions arise. For example: Is it socially acceptable that facial recognition is used in public places? For what purposes? Who and how can guarantee a use that respects the principles of necessity and proportionality? Which is the role of Governments, society and the other stakeholders? These questions are not answered by the GDPR. Well aware of these dilemmas, the Commission determines that it "*will launch a broad European debate on the specific circumstances, if any, which might justify such use, and on common safeguards'*.

BEUC welcomes the fact that the Commission wishes to have a broad and inclusive debate on the use of these systems. However, in our view, this debate must not to be limited only to the specificities identified by the Commission (remote identification in public spaces). There are actually many other uses of biometric data that should be subject to a public debate as their effect can be irreversible for society and future generations. For example, more attention should be paid to the risks arising from the use of biometric data of vulnerable subjects, such as children. A recent study took the processing of children's biometric data as paradigmatic example underlying that '*that closer attention must be paid to the actual social contexts in which data relating to children comes to affect their lives through AI practices'*[23]. In this sense, we emphasise that all biometric systems and all collections of biometric data, regardless of being for identification or for authentication purposes, can lead to problematic outcomes. We would therefore recommend to apply heightened safeguards also to seemingly less intrusive biometric techniques.

[22] In fact, there are simple biometric identification systems which compare individual physical or behavioural characteristics with the information stored in the system in order to find a match for the purpose of identifying the person. Such systems – which seem to be out of the scope of the White Paper - differ from those which embed machine learning techniques which – in addition to data collection and combination - allow the system to learn, react and adapt its endeavours on the basis of its findings. These latter technologies are defined in the White Paper as 'remote biometric identification'.

[23] Velislava Hillman, Nick Couldry, Elettra Bietti, Gretchen Greene, Response to the European Commission's communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence (White Paper COM 2020-65).

In order to tackle these problems, **we recommend the Commission to**:

- Ensure **full compliance with the GDPR** and strong application of key principles such as, transparency, data minimisation and purpose limitation.
- Ensure that individuals can remain in control and exercise their rights when they are not directly interacting with the technology (e.g. when a consumer is walking down the street and is inadvertently captured by a facial recognition system installed in a shop or an interactive billboard).
- Develop a **risk assessment** system and enable possibilities for **independent testing** for accuracy and unfair bias.
- Biometric technology should never be deployed without a **prior impact assessment** (not only limited to data protection impact) and consultation with the competent supervisory authority.
- Clear **red lines** must be established to limit or, where appropriate, prohibit the use of biometric technology for specific purposes or in specific situations (e.g. to monitor children in schools) where the risk for people's rights and freedoms would be too high and the impact of this technology would be detrimental to the individual or to society as a whole.
- When it comes to consumer identification via biometric data (e.g. to enter a venue for a concert, to access an online banking account, or to unlock a mobile device) the consumer should, as a general rule and taking into account security risks, be provided with the possibility to **choose another identification system** instead that does not require the processing of biometric data.
- The use of biometric identification technology, such as facial recognition, should not be 'normalised' and widely deployed given the serious data protection and privacy implications and risks of such technology.

END