BEUC The European Consumer Organisation

The Consumer Voice in Europe

AI RIGHTS FOR CONSUMERS

Contact: David Martin – 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-2019-063 - 23/10/2019

Why it matters to consumers

Artificial intelligence (AI) is changing the way in which consumer markets and our societies function. AI evokes big promises to make our lives easier and our societies better. It is powering a whole range of new types of products and services, from digital assistants to autonomous cars and all sorts of 'smart' devices. All this can bring benefits for consumers, but the widespread use of AI also raises many concerns. Consumers are at risk of being manipulated and becoming subject to discriminatory treatment and arbitrary, non-transparent decisions. It is essential to make sure that consumers have strong and tangible rights to defend themselves when necessary and which empower them to reap the benefits of the digital transformation of our societies.

Summary

Ethical guidance – such as the principles published in June 2018 by the High-Level Expert Group on artificial intelligence – is not enough to ensure consumers have effective rights and can have confidence in emerging new technologies. The existing legal framework is not sufficient and legislation is needed.

In this paper, we outline a set of AI rights for consumers, which relate to principles that ensure a fair, safe, and just society and set to guarantee a high level of consumer protection. These rights should be concretised and translated into enforceable rules so that AI serves consumers and does not harm them. Legislators must make sure that AI products and services are safe and that risks – including discrimination, loss of privacy, loss of autonomy, and lack of transparency – are avoided. In particular, consumers should have the following rights:

- 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

Introduction

The 21st century will be known as the digital era: consumers' lives are increasingly dominated by their interaction with products and services that are interconnected and increasingly automated using algorithms. The shift towards algorithm-based decision making (ADM[1]) and artificial intelligence (AI) is changing the way in which consumer markets and our societies function. Although the opportunities AI offers for consumers can be significant (e.g. potential to power a whole new range of innovative services and products), strong consumer rights are necessary to address the risks associated with the digital transformation and to ensure that consumers and society as a whole can reap the benefits of it.

Markets can only function if there is consumer trust in the underlying technologies. As regards algorithmic decision making, there are new consumer and societal challenges that deserve attention by policy makers. Do we want to live in a society where people are constantly scanned, sorted, categorised, and tracked, mostly without their knowledge? For example, algorithms used for facial recognition can have serious impacts on people's lives and challenge our current safeguards against discrimination and unfairness. The AI consumer rights we establish in this paper should be seen as safeguards against these and other potential abuses.

Such consumer protection is necessary to protect the autonomy and dignity of people but should also be seen as an AI innovation enabler in the internal market. AI can empower, strengthen and support consumers if they are able to be in control and make it work for them rather than the other way around. In view of the European Commission's plan to propose legislation to regulate artificial intelligence within the first 100 days of the new mandate, this document outlines a set of specific AI rights for consumers, which relate to fairness, transparency, accountability and other principles that ensure a fair, safe, and just society. Ethical guidance alone is not enough to ensure consumer confidence in emerging new technologies. Therefore our proposal for AI rights should be concretised and translated into law. Existing legislation, such as the General Data Protection Regulation (GDPR), does not provide enough protection for consumers.

A horizontal legal framework setting the main principles to regulate AI and ADM systems and a revision of relevant sector specific legislation (e.g. the Product Liability Directive) are needed. New rules should follow the general principle that the higher the potential adverse impacts of the use of algorithmic decision making and AI technology, the stronger the appropriate regulatory response must be. Particular attention should be given for example to the use of biometrics technology, such as facial recognition, which is quickly becoming the new norm for user identification, authentication and access control.

As risks and benefits are not limited to the private sector, measures must also be taken in the public sector. Governments are in a privileged position of power and their decisions to use ADM systems can have a major impact on citizen's lives or easily interfere with their fundamental rights. Risks associated to privacy, fairness, or discrimination are exacerbated when, and this is a major difference to the private sector, citizens cannot simply choose another provider: For example, if governments ignore privacy rights when rolling out AI-services, surveillance may become an inescapable part of citizens' lives. Predictive analysis used by employment services or by the police may lead to or amplify existing discrimination.

[1] For the purpose of this paper, algorithm-based decision making should be understood broadly, including cases in which a significant part of a decision-making process is carried out by a machine, such as credit ranking (where the final decision lies with the bank). Artificial intelligence is a narrower concept, where self-learning machines perform tasks which typically require human intelligence.

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.

The modern economy is based on data-driven markets, where it is increasingly difficult for consumers to understand business practices. Consumers should always have a right to get a clear picture about algorithmic decision-making processes that may negatively affect them or, at a larger scale, have the potential to cause harm to the society. Hence, consumers should have a right to information, a right which is anchored as a key principle under the EU Treaties (Art 169 TFEU). This right should encompass both transparency about the fact that automation takes place and about how it works, such as how information is filtered and presented.

Even more transparency is required where algorithmic-decision making can have significant[2] consequences on consumers lives or bear serious risks for them, such as credit scoring. Before an automated decision-making process is carried out, consumers should have a right to be informed about *what* data will be processed by *whom* and for *which* purpose. They should be informed about the functionality of the system, its significance and its consequences. Importantly, in cases where decisions have a significant impact on consumers lives, consumers should have a right to object to algorithmic decision-making and to request human intervention. Thereafter, consumers should have a right to request an explanation, hence, to learn how a machine has arrived at its result, and a right to express his or her point of view and to object the decision. These rights should not depend on the processing of personal data as this is the case under EU data protection rules[3] but apply to the use of any data for the decision-making. This is why the GDPR cannot offer sufficient protection in the context of AI. It should also apply where ADM is not fully automated but used as a preparatory or supportive tool for a person who has the final say.

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.

Whether an algorithm-based decision is accurate, fair, or discriminative can only be assessed if an appropriate system for control is in place. Such a control system must be multi-layered and incorporate multiple elements to minimise the risks of relevant ADM processes. It must be a minimum requirement that there is control by those who have access to the data basis and can understand which and how decision criteria are applied. 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. The monitoring of ADM processes by the company who applies them must be ensured on an ongoing basis. The higher the potential risks, the greater should the accountability measures be which the company must put in place. It could comprise ADM impact assessments, documentation, internal audits or transparency measures for the users.

[2] The significance criterion is laid down in the General Data Protection Regulation on several occasions, for example, as regards the necessity for a data protection impact assessment (Art 35) or the user rights in case of automated decision making (Art 22).

[3] Art 22 of the GDPR sets out that the data subject has the right not to be subject to automated decision-making. However, this right is restricted to fully automated processing of data and does not apply in a number of cases, such as when the decision making is based on uses' consent.

At the same time, companies must put in place measures to allow for external control of their ADM systems. This can be done though technical options, such as interfaces, which give data access to competent supervisory authorities. Such authorities, which should be well-equipped and possess the necessary expertise, should have the competence to inspect ADM systems and to assess the relevance and significance of algorithmic decision making (content control). For example, authorities should have the competence to check whether a scoring software has the potential to discriminate a certain group of people. The higher the risks, the greater the need for regulatory control and intervention.

A comprehensive ADM risk assessment system must be developed. To define the level of risk of an application, the relevant competent supervisory authority should draw up a list of criteria to define its potential to cause harm or damage to individuals and/or society. Depending on the level of risk, the authorities should have the competence to impose the necessary documentation, certification, or transparency measures. For those applications that present the highest levels of risk, ex-ante scrutiny procedures (e.g. pre-approval before market deployment, publication of impact assessments) should be put in place. As an ultima ratio measure, authorities should be able to ban the use of certain ADM processes or parts/components thereof. Authorities should have the right to terminate ADM systems in case they pose a significant risk to individuals and society that is not properly managed by the company/public service operator who uses ADM.

Right to Fairness

Consumers should have a right that algorithmic decision making is done in a fair and responsible way.

The principle of fairness relates to many aspects that consumers' lives, such as equality of benefits, avoidance of risks, protection from exploitation. It also includes general welfare considerations. As regards algorithmic decision making, there are several aspects of fairness that must be addressed in the form of AI rights for consumers. Most importantly, consumers have a general expectation and thus should have a right that algorithmic decision-making is done in a fair and responsible manner. 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 intention of what do to with the result. The outcome should be fair too, hence the result should not lead to an unjust treatment or behaviour. The latter 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 predicting analysis. Modern rules should therefore focus on processing *results*, to prevent unfairness, deception and manipulation stemming from algorithmic inferences and mathematical-statistical methods.

Businesses practices must be fair too: the use of algorithms should never lead to consumers being deceived or impaired in their freedom of choice. Their expectations should be protected and their weak position with regards to the business be respected. However, current rules on unfair market practices do not sufficiently consider consumer detriment associated with algorithmic decision making. Questions of fairness should also be seen under the aspect of general welfare considerations. A lack of fairness can foster greater societal asymmetries, lead to unequal benefits for citizens or could even lead to certain groups of people being exposed to higher risks of poverty. The deployment of AI systems must thus consider their impact on the well-being of citizens.

Right to Non-discrimination

Consumers should have a right to be protected from illegal discrimination and unfair differentiation.

If the outcome of an ADM is potentially unfair, systematic discrimination may follow. AI-driven decision making can lead to discrimination at several levels: due to the use of biased databases or lack of data relevance, a profiling process may have reached an incorrect prediction, hence wrongly classified individuals as having certain characteristics. When aggregated, such errors could disproportionately harm certain groups. Even where the outcome is correct, classifications may lead to adverse societal effects: for instance, an individual correctly classified as "poor" being automatically denied access to a service or prevented from receiving certain offers for medical treatment. There are many forms of potentially unfair differentiation, which may disproportionately harm certain groups in a society, such as price discrimination online.

It is also feasible that those who use algorithms may intentionally try to achieve a discriminatory outcome in order to exclude certain groups of persons from services.

Many situations cannot be properly tackled using anti-discrimination laws, as they traditionally focus on discrimination based on protected characteristics, such as skin colour. AI system can use classes and categories for differentiation that do not (directly) relate to protected characteristics. The higher the societal risk of such proxy discrimination, the greater is the need for regulatory safeguards and public scrutiny.

Right to Safety and Security

Consumers should have a right that AI-powered products are safe and secure throughout their lifecycle.

Consumers expect that their goods, digital content products, or services are safe and secure and are kept that way throughout their expected lifetime. For example, advanced robots or IoT products may eventually malfunction or act in a way which was not foreseen at the time of production. At stake are not only the protection of the individual or their property but also the public and collective interest of a society to live in a safe environment. Consumers should be able to trust that new technologies are safe and secure, that producers minimise risks, and that public authorities ensure a proper regulatory oversight. Relevant legislation, such as the EU directives on product safety and product liability fail to adequately deal with of the problems related to connected products or software, and related issues of data or IT-security, and therefore need to be expanded in scope and updated[4]. Legislation must ensure that there is a specific security standard in place for products with embedded software, particularly those whose functions are based on algorithmic decision making. Any legal reform must consider the dynamic nature of software components. Modern devices need performance and security-updates, and the general public expects that those updates are delivered throughout the lifecycle of the product.

[4] See BEUC position paper on the review of Product Liability rules (BEUC-X-2017-039)

Right to Access to Justice

Consumers have a right to redress and public enforcement if risks associated with artificial intelligence materialise.

Greater protection in terms of safety, non-discrimination, or fairness will be vital before consumers can trust ADM-powered products and services to play a greater role in their lives. 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. In this respect, current rules on product liability should be brought up to date to deal with problems created by new technological advancements, including automated and autonomous products, robotics, or cloud technology, hence also software products or services that may cause consumer harm. It must be ensured that burden of proof rules or liability exceptions do not hamper the victims' access to justice. As a rule, any professional in the product supply chain should be responsible to ensure that the product is safe and should be held liable for defects when their activities have affected the safety of the final product which was then placed on the market.

Consumers should also trust that rogue companies face dissuasive sanctions and that authorities take actions if harm occurs. The right to access to justice also comprises the support by market watchdogs, such as consumer organisations. They must be adequately empowered and equipped to represent the collective interest of all affected victims.

If something goes wrong, consumers need protection by private and public enforcement. Both approaches have their own merits and it must be made sure that there is a dynamic and solid connection between them, such as the possibility to rely on public enforcement decisions for follow-on legal actions by private entities.

Right to Reliability and Robustness

Consumers should have a right that AI powered products are technically reliable and robust by design.

The more autonomous machines become, the more important it is for users to trust the system being reliable regarding their performance, accuracy, and robustness throughout their life cycle. High data quality 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, it must be ensured that companies use proper training data sets and that data quality mechanisms are put in place to avoid biases, errors, and other irregularities. Review and validation processes should become a common industry standard. It should also be ensured that AI systems are resilient to attacks and that safety protocols and fall-back plans are available, including options for process termination.

Technical robustness also implies that attention must be paid to the context in which the application is used and the target group by which it is used. For example, it must already be considered, in the design phase, whether the system will be used in the public or private realm or whether users may be in a situation of vulnerability or have specific needs.

For more information
BEUC Position Paper ''Automated Decision Making and Artificial Intelligence: A consumer perspective'' (BEUC-X-2018-058)
Federation of German Consumer Organisations – vzbv: Factsheet ''Artificial Intelligence: Trust is good, control is better''

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