The Consumer Voice in Europe

AUTOMATED DECISION MAKING AND ARTIFICIAL INTELLIGENCE - A CONSUMER PERSPECTIVE

BEUC Position Paper

Contact: **Christoph Schmon– 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 • consumers@beuc.eu • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2018-058 - 20/06/2018

Why it matters to consumers

Consumer's lives are dominated by products and technologies which are interconnected and increasingly automated and intelligent. The shift towards the use of automated decision making based on algorithms for commercial transactions will change the way in which consumer markets and our societies function.

New products and services will be tailored for its users and hold the promise of bringing more convenience and efficiency. However, policy makers need to be fast and ambitious to make sure that products are safe and law-compliant by default and that risks, such as discrimination, loss of privacy and autonomy, lack of transparency, and enforcement failure are avoided.

Summary

The shift towards automated decision making (ADM) and artificial intelligence (AI) will change the way in which consumer markets and our societies function. In order to make sure that consumers reap all the benefits of this transformation and in order to avoid harm, policy makers should take the following recommendations into account:

- The concentration of data in the hands of a few private businesses should be avoided so competing companies can provide innovative products and services based on ADM and AI solutions for consumers.
- AI based products and services must be user-friendly and legally compliant by default. Discrimination and lack of transparency or privacy should be avoided.
- There should be a general duty of Member States to ensure adequate sanctions, reparation and compensation for victims harmed by discriminatory and/or illegal ADM practices.
- There should be the rights to object automated decision making and to contest the decision of automated decision making. Users should have a right to transparency on which parameters offers are based and how the machine has arrived at its result.
- Policy makers should analyse whether horizontal EU consumer law is fit for the challenges of a data economy. It should also be examined whether sector-specific rules regarding health, financial, and energy services are fit for purpose.
- An AI Consumer Action Plan and necessary legislative changes for adapting the consumer protection framework to the new market reality should be established asap as a key priority of the new European Commission.
- Artificial Intelligence must be developed and used in full respect of EU data protection rules, considering the principles of fairness, transparency, purpose limitation, data minimisation, accountability and privacy by design.
- It should be a general principle that companies must introduce effective mechanisms for auditing AI's use of data. ADM auditing should be carried out by independent third parties or specific public bodies.
- The EU should adopt modern liability rules for situations where consumers are harmed by unsafe or defective products, digital content products, and services. It should also be should be analysed whether the EU safety legal framework is fit for practice.

Table of Contents

---°--

1. Introduction

The 21st century will be known as the digital era: consumers' lives are increasingly dominated by their interaction with products and technologies that are interconnected and increasingly automated. At the centre of the digital economy is the production of vast amounts of data through platforms, social networks, and machines that consumers put in their homes, in their pockets, or in their cars.

In this digital revolution, algorithms play an increasingly important role: more and more tasks and decisions are entrusted to self-learning machines which execute orders autonomously. Until recently, machine learning was based on fairly limited sample data sets. But big data and the exponential increase in computer capacity have led to the emergence of a powerful processing machine which has changed the equation: Big Data analytics. Relying on machine learning algorithms, Big Data analytics help managing this vast amount of information while machine-learning applications help transforming such information into useful and profitable outcomes.

Thanks to automated decision making (ADM[1]), software and applications can perform complex functions. Some machine-learning applications perform tasks typically associated with human beings while showing a certain level of intelligence, hence the capability to learn, to perceive, or to reason (Artificial Intelligence – AI). Decision-making based on algorithms have not only become an area of strategic importance and economic development but are going to become part of the everyday life of consumers, and change the way in which many consumer markets, products and services operate. Whether consumers give instructions to a digital assistant, request the fastest track from a navigation programs, or use smart accounting apps: through self-learning algorithms, those services will provide a targeted response addressing those instructions.

AI and ADM are about to transform entire economic sectors. For example, traditional financial firms and FinTechs are increasingly integrating AI into their services. Robo-advisors provide investment services, chat bots interact with customers online and help them to manage their budgets, biometrics prevent payment fraud and offer convenience, payment transaction monitoring fights against money laundering, and there are automated creditworthiness checks and credit decision. The insurance industry is already using data input and monitoring systems to offer discounts on premiums or to create tailored customer packages. AI has a huge potential to cut costs and boost benefits of financial service providers. But one important question remains unanswered: will those benefits be passed on to consumers?

Many other areas, such as the food, electricity, or health sectors will adapt to this new technology. More and more products such as connected vacuum cleaners, automated cars, automated consumer advice in financial service and other sectors such as consumer credit rating, demonstrate why automated decision making and AI are becoming a reality that matters to consumers.

[1] For the purpose of this paper, automated 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 narrow concept, where self-learning machines perform tasks which typically require human intelligence.

The ongoing shift towards algorithm-based decisions is changing society as a whole. Policy-makers and public institutions need to be fast and ambitious to make sure that consumers reap the benefits that this transformation can bring. At the same time, they need to prevent the numerous risks that will appear and address problematic issues for consumers.

In its recent Communication on Artificial Intelligence[2], the European Commission has recognised the need for action. However, it is regrettable that there is no clear commitment to update the EU's product safety and liability rules or other relevant consumer rights laws to ensure they are fit for the AI era.

By participating in the Commission High-Level Group on Artificial Intelligence and Expert Group on Liability and New Technologies, BEUC will be vocal and try to ensure that the European Union will take swift policy measures against, and focus research efforts on, potential risks of AI for society and consumers. Similarly, the European Parliament states in its report on civil rules regarding robotics[3] that the rules on product liability are not sufficient to deal with robotics and AI. It stresses the need for new legislation to address relevant questions and concerns.

2. Potential Benefits and Risks

2.1. Optimisation, Convenience, Performance boost

The shift towards AI and ADM promises to bring a convenience boost for consumers: in the future, there will be intelligent applications to make their lives easier or help them save money.

A typical example is the use of AI/ADM to increase the efficiency of online search and to power digital assistants. Big technology companies have recognised the opportunity in competing for that sector and many have already put their digital assistants on the market (Apple's Siri, Amazon's Alexa, Google Assistant, Microsoft's Cortana).

Another paradigmatic example could be applications that help consumers reduce their energy consumption. In this sense, AI could help optimise the household's electricity consumption based on automatic learning about the usual consumption of each individual household, and thereby increase the comfort in people's homes and make energy bills more affordable.

Other popular applications already on the market today will bring convenience by offering fully autonomous machines, may this be the self-driving car or the automated household robot. AI-powered applications should also help the elderly or people with disabilities have better access to services and enhance social inclusion.

Thanks to big data analytics, the ocean of data collected by companies can be used to personalise services and content in a way in which it was not possible before.

From scientific research to medical diagnosis, and precision engineering to surgery, ADM and AI could also lead to promising benefits in how all these activities are performed. AI technologies are increasingly being used by scientific and medical research communities to progress faster and innovate better in many areas.

[2] COM(2018) 237 final.

[3] Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)).

Consumers should have a right to fully benefit from technological advancements and innovation.

2.2. Associated risks

Besides the numerous benefits machine learning can bring, there are several risks associated with these new technologies which require careful attention and analysis on a broad political level.

In this sense, algorithms used by business gain control over how products and services function and have an influence over the inclusion and exclusion of people and information. This may create situations of information and power asymmetries which impede consumers from taking informed decisions.

Engaging with such AI/ADM-based products and services poses a related question about how to ensure that consumers have the necessary digital literacy to use or engage with these products and services.

Other risks include the fact that decision-making by machines may lead to discrimination of certain groups of people or provoke lock-in effects, negatively impacting competition in the market.

Other important challenges for consumers include how to protect their rights, in particular with relation to data protection, and whether current consumer protection rules are fit for purpose. Finally, it must be discussed who is responsible if something goes wrong (algorithmic accountability) and who has the power to control the ones who have the power over algorithms (ADM auditing and control).

These pertinent questions are discussed below.

3. The algorithm blackbox – market transparency

3.1. Can consumers take informed decisions?

Whenever consumers interact with smart technologies, they are confronted with a wave of personalised and targeted content, often without even knowing it. User profiles and algorithms are invisible to users who can usually not opt out. Consumers do not need to enter a specific market context (online shop) for advertising to work. Smart algorithms choose the time when it is best to approach the consumer and decide about the offers consumers receive. Big data analytics enable companies to analyse the behavioural pattern of users and to predict emotional responses needed to make the user act and which stimuli can be used to provoke such responses. Consumers have no way of knowing about the profiles building up about them and have no information about the underlying method used to target and influence them.

The increased personalisation and targeting of services and information could diminish the choices of users and hamper their ability to find information which they consider meaningful to make an informed decision. The bigger the individual's dependence on these technologies to make an informed decision, the less likely they will have a real choice.

The underlying technical systems and algorithms used by business are not exposed to public scrutiny and are usually protected by Intellectual Property rights and trade secrets, giving rise to the ‘algorithm blackbox’. Due to the lack of transparency of these algorithms, users do not know how their personal data has been analysed, to what end and by whom, or why they received a specific content or response from the AI/ADM service or product.

In such an environment, consumers are highly vulnerable to be manipulated by businesses into a specific choice of purchase. This may lead to concrete economic and social harm, when for example a credit or insurance is denied to the consumer based on irrelevant and discriminatory elements, such as gender, race, religion, or postal address.

Other examples of harm may stem from the use of personal data by companies which show a certain behavioural pattern of consumers. For example, when it comes to smart meters, algorithms learn what is happening in the house which then could lead to behavioural profiling, targeted advertising and possibly also to determining behaviour that might be used to evaluate the creditworthiness of the consumer.

Physical harm can also exist, for example in cases where big data analytics use non-contextualised information to influence consumer behaviour when it comes to health-related decisions, for example such as giving up smoking. The same holds true in the case of mHealth apps, which collect information about users and merge health content and commercial content, ultimately nudging consumers in a certain direction without them knowing it.

3.2. Functioning of markets and application of EU consumer law

The impact on business practices and the consequential functioning of markets with these new technologies needs to be assessed.

We need to ask the fundamental question if the concepts and paradigm on which European consumer law is built, such as consumer empowerment through information and transparency, consumer protection of the circumspect person who can make an informed choice by comparing offers, can stand the fitness test?

For example, is it realistic to protect consumers through information provided by business to them, when this information is individually targeted at them depending on their profile established by the business? How will consumers be protected when they face discriminatory results of AI based ADM? How can consumers compare offers and prices and what is the reference indication for a fair price when nobody except data brokers have access to price information?

New forms of potentially unfair advertising and other practices need to be addressed. Consumers will often be unaware of restrictions when it comes to commercial offers or they will not be aware that the price of a product is determined based on their user profile (personalised pricing).

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?

Clearly, the idea of autonomy and free decision-making is at stake where consumers have no understanding of how the market works or how the offers they receive have been generated. Depending on how algorithms work, price ranking may be opaque, making the comparison of offers very difficult for consumers. Consumers should be empowered to understand how information is organised and presented and which criteria have been used to rank information.

Similar problems arise when it comes to the purchase of products or services which use or run on algorithms. EU rules which deal with pre-contractual information requirements, such as the Consumer Rights Directive, are out of date to deal with such products or services. Under current rules, consumers have the right to receive essential information about the product or service, for example its characteristics or its price. However, EU law does not set out information items on the ADM process, individual or dynamic pricing. This is of relevance not only for digital services but also for products that run on ADM processes for their functioning. It is worth noting that the proposed Directive on the modernisation and enforcement of consumer law[4] suggests the inclusion of new information pieces related to the parameters of ranking. However, there is no obligation to inform the consumer about the relative importance of ranking parameters and the reasons why those criteria were chosen. Information about the underlying algorithms are not included in the transparency standard.

Another example is the Unfair Contract Terms Directive. The current rules are formulated in an abstract way, without giving due consideration to the specificities of data processing, big data, or algorithms. On top of this, the Directive does not sufficiently address the common practice where companies use a general disclaimer to remove any liability in case of consumer harm. Other pieces of legislation, such as the Price Indication Directive simply do not apply to digital services and do not take into account flexible offers based on algorithms. This is relevant because consumers should be able to compare prices effectively.

Burden of proof is a key requirement for the enforcement of consumer rights, for example to invoke legal guarantee rights under the Sales Directive or to establish liability under the Product Liability Directive. However, the more complex the product is, the more difficult it will be for consumers to make their case.

These examples demonstrate the important role of consumer law in developing an AI legal framework. Consumer law can help ensure that consumers get accurate and reliable information about the nature of the business model and the nature of the specific offer. It can prevent exploitation and can tackle transparency issues. While data protection provides the limits for the collection and processing of consumer data for the purpose of delivering AI solutions, consumer law can make sure that consumers understand the implications of such technologies and the outcome of the decisions made by machine-learning technologies.

On top of that, consumer law can help Artificial Intelligence take off in the European Union. If there is no transparency around the use of products which run on algorithms, consumers' trust in AI products will be negatively impacted.[5]

[4] COM(2018) 183 final.

[5] For example, a recent German study has shown that only 15% of consumers would use virtual assistants, such as Alexa or Siri, for online shopping.

What is needed is a detailed mapping and careful evaluation of the entire EU consumer law acquis, as well as sector-specific rules, in particular legislation on health services, financial services and energy services to check whether these legal frameworks are fit for the AI/ADM age. It is disappointing to see that the European Commission, in its recently published Strategy on Artificial Intelligence, does not recognise the urgency of doing this crucial exercise for consumers.

4. Discrimination

Another important issue that stems from the rise of AI/ADM is related to the categorisation and discrimination of consumers. Consumers, based on their profile, are assigned to market segments with an increasing degree of precision. Such categorisation may prove problematic in several situations. For example, there is a problem if the profiling process has reached the wrong outcome and a wrong profile is applied. This could be because of inherent errors in the computing technique of the statistical analysis or biased databases that may make the system reach false positives or false negatives.

Discrimination can occur where the data input on the consumer is not relevant enough to reach a correct conclusion. The consequences of such automated decisions can be severe: the user may be deprived of a service or denied access to information.

It is also possible that those in control of algorithms intentionally try to achieve unfair, discriminatory, or biased outcomes in order to exclude certain groups of persons. One example would be where profiling indicates that an individual is highly likely to belong to a certain group in society and therefore an invitation to buy a service is not provided or offers from that individual are automatically rejected. The societal implications can be severe.

In addition, digital records of human behaviour can reveal highly sensitive data, not only in terms of preferences, but also regarding sexual orientation, age, gender, and religious and political views. That way, the one in control of such information can assess what triggered a certain behaviour, for instance addiction to drugs or gambling, low or high income, a certain medical condition, or certain mood, and use this to his advantage, for example by receiving personalised products the morning after the user has lost his job or if the programme predicts that the self-esteem of the user is at its lowest.

This type of categorisation leads to a treatment that is different according to the user. Individuals will receive different kinds of prices or different kinds of special offers and deals because they are associated with a certain group, while others do not have access to the same offers. For example, people who are categorised as rich may receive ads on a breakthrough medical treatment just because they are deemed to be able to pay for it. Others may be excluded from services as a “high risk” group, based on their nationality or religious beliefs.

5. Challenges for competition: lock-in effects and exploitation of consumer biases

The expansion of AI/ADM-based technologies and the widespread use of Big Data create new market dynamics. Firms have started investing to incorporate these technologies into their business models and management systems. Yet whether access to relevant data can be ensured or not will be the key strategic element in a business plan. Today huge data sets are brought under the same corporate umbrella raising concerns about how firms in downstream markets can benefit from AI and provide new services to consumers.

There is therefore a risk that consumers could be held hostage of a lock-in effect, getting access only to specific products from specific market players that have the capacity to use algorithms in the context of ADM, and hence get the upper hand in engaging with the consumer in a more timely and relevant manner as compared to others.

By contrast, market players that do not have the means to access data and invest in such technology will in time be edged out. Due to the lack of competition in such market, there is an increasing risk of limitation of choice for consumers, higher prices and less quality of both the product or service and the quality of the algorithms used as well. For these reasons it is necessary to identify solutions to limit reduce the risk of concentration of power over information.

Another challenge of AI relates to the opportunities it brings to allow firms to exploit consumer biases and vulnerabilities. Through machine-learning and algorithms programmed to provide prices of consumers based on their online behaviour, consumers might lose their ability to access prices based on competition forces (price discrimination). The combination between tracking-price technologies and the data provided by consumers as input to the machine-learning process, would allow companies to establish consumption patterns and therefore offer the exact price a consumer would be able or willing to pay. This may be particularly relevant where consumers are particularly vulnerable because they have less access to information or alternatives due to less economic means or in situations where they need to buy a certain product or service and are therefore less price sensitive, for example a medicine or a health insurance. The additional knowledge provided through AI may therefore disproportionately and negatively affect certain groups of consumers.

Similarly, those algorithms can be programmed to collude through the automatic adjustment of prices based on price monitoring technologies. For example, the European Commission's final report on the e-commerce sector inquiry indicates that automatised adjustment of prices is a growing tendency among retailers.[6]

[6] The report notes that: "A majority of retailers track the online prices of competitors. Two thirds of them use automatic software programmes that adjust their own prices based on the observed prices of competitors. With pricing software, detecting deviations from 'recommended' retail prices take a matter of seconds and manufacturers are increasingly able to monitor and influence retailers' price setting. The availability of real-time pricing information may also trigger automatised price coordination." European Commission (2017), Final Report on the E-commerce Sector Inquiry, paragraph 13.

This trend may lead to various possible scenarios: first, the homogenisation of prices by means of collusion or, secondly, to personalised pricing but happening on a massive scale. In one way or the other, consumers risk facing non-transparent markets, higher search costs and welfare losses. In this regard, it is necessary to ensure that different regulators act within their competences (e.g. consumer protection, data protection and competition) to address those challenges and ensure that these technologies are designed to respect EU laws e.g. by making companies accountable for the programming of their algorithms in a way that breaches their legal obligations. Particularly in case of bundled offers, a smooth cooperation between authorities, such as consumer and data protection authorities, will be necessary.

Policy recommendations to address the challenges of algorithm blackbox, discrimination, and competition:

- Artificial intelligence poses a range of challenges to policymakers. Lawmakers must ensure that the potentially negative impact is avoided through policy measures. It is important to recognize that, alongside the huge benefits that AI offers, there are numerous risks associated to it.

- Lawmakers must ensure that the concentration of data in the hands of a few businesses is avoided so competing companies can provide innovative ADM and AI solutions for consumers therefore guaranteeing consumer choice.

- Regulators must ensure that firms design their ADM technologies in full compliance with EU laws, in particular with consumer protection, privacy and competition rules.

- Policy makers should analyse whether EU consumer law is fit for practice when it comes to technologies based on ADM. This includes the Directives on Unfair Commercial Practices, Unfair Contract Terms, Consumer Rights, Product Liability, Sales of consumers goods, and Price Indication.

- AI products and services must be consumer-friendly and legally compliant by default. They must be designed so as to avoid undue discrimination, invasive marketing, or loss of privacy. Public research and stakeholder discussions are necessary to address the question of ethics of AI. Guidance on AI and automated decision making should be developed, focusing on the repercussions of AI on fundamental rights, non-discrimination, consumer protection, and transparency.[7]

- There should be a general duty of Member States to ensure adequate sanctions, reparation and compensation for victims harmed by discriminatory and/or illegal ADM practices.

- Users should have a right to transparency: there should be a general information obligation for companies providing services to consumers that are based on automatised processes such as those based on algorithms. The obligation should explain how the logic of the algorithm functions, including how the information is organised and presented to consumers. For example, the criteria used to rank or display the information should be listed. Consumer should always be informed about the existence of personalised or automated pricing in a user-friendly way.

[7] For example, the Mortgage Credit Directive (Art 18) anchors an information requirement, obligating the creditor to inform the consumer without delay of the reject and whether the decision is based on automated processing of data. Where the rejection is based on the database consultation, the creditor has to inform the consumer about the result of such consultation.

- There should be a right to object automated decision making and to contest the decision of automated decision making.

- There should be an investigation into whether and under which circumstances a consumer should have a right to be informed about how the machine has arrived at its result, for example the reasons for rejecting a consumer request or why the trader does not process the consumer request if this decision is based on ADM.

- Policy makers should also examine sector-specific rules, particularly health, financial services, and energy services legislation, and decide whether they are fit for purpose and take into account the dimension of ADM. The views of relevant stakeholders, in particularly consumer organisations should be taken into account.

- There is an urgent need to clarify the liability of companies which use algorithms or artificial intelligence technology. Disclaimers which generally exclude any form of liability should be considered unfair in all circumstances. EU legislation on product liability should be reviewed as a matter of priority.

- An AI Consumer Action Plan and necessary legislative changes for adapting the consumer protection framework to the new market reality should be established asap as a key priority of the new European Commission.

6. AI and Data Protection

Artificial Intelligence is powered by filtered and personalised information. This information is collected through all sorts of channels: social media platforms, the consumer's favourite news sources and the mobile apps they use. At the development stage, data is used to train machines and enable them to develop their learning capacities. Once in action, AI continues to need data, be it to simply perform the task it has been programmed for and produce an output, and eventually, to continue learning and adjusting in the process. Much of that data is personal data. The volume of the data used, its sourcing, the importance of data accuracy, the complexity of the data processing operations and, in some cases, the unpredictability and opacity of the outcome, all raise serious risks and challenges from the point of view of data protection and privacy.

6.1. The role of the General Data Protection Regulation (GDPR)

A basic starting point is that AI must be developed and used in full respect of the data protection rules. The General Data Protection Regulation (GDPR) applies whenever personal data are used in the context of Artificial Intelligence.

However, there are many questions related to the meaning, practical application and limits of some of the fundamental principles of the GDPR such as the fairness and transparency of personal data processing, data minimisation, purpose limitation and accountability:

- How can we ensure that consumers remain in control of their data and that the data collected for one purpose are not re-used for something completely different?
- How do we ensure meaningful information for consumers regarding the usage of their data and its consequences, especially when consumers' informed consent is required?
- Does the GDPR give consumers a right to receive an explanation of AI powered decisions?

- How do we ensure that AI only uses data that are lawfully obtained, adequate, relevant and limited to what is necessary for the purpose sought?
- How do we prevent arbitrary discriminatory treatment and ensure that there is no built-in bias in automated decision making?
- To what extent does AI development and use fall under the realm of data processing for scientific research purposes?

It is necessary to look at all these and many other questions in detail to analyse the privacy implications of Artificial Intelligence and ensure that it is developed and used in a way that is respectful of consumers' fundamental rights and the core values of our society. Further to this, enforcers need also to look at the enforcement of data protection and consumer protection law in tandem as these both areas of law seek to empower the user as a data subject (in relation to the collection and use of his or her personal data) and as a consumer (in relation to the protection of his or her economic interests).

Three issues are particularly relevant from a consumer viewpoint:

THE NEED FOR TRANSPARENCY AND INFORMED CONSENT

Artificial Intelligence often entails very complex technical processes which are hard to explain and understand for those who do not have the knowledge and expertise required to work in the field. Sometimes even those involved in the development and use of AI can struggle to explain and predict the functioning and the outcomes produced by AI.

Consumers cannot give valid consent for the use of their personal data if it is not clear for them how it will be used and for what purposes. As explained above, the algorithms that power AI often operate inside 'black boxes' with little transparency. Meanwhile, the GDPR has strict obligations regarding the information that must be provided to users when their personal data is processed.[8] These obligations must be fulfilled not only when users' consent is requested, they also apply no matter the legal ground used for processing the data (e.g. based on legitimate interest or for the performance of a contract).

According to the GDPR, users must receive easy to understand information, among other things, about the categories of personal data that are processed, the purposes of processing, the recipients or categories of recipients of the personal data and, if there is automated decision making involved, meaningful information about the logic involved and its possible consequences.

It is hard to see how these obligations will be met unless much more transparency is injected into AI systems and processes. Additional efforts are necessary to increase algorithmic transparency and explain to consumers how AI systems and processes/products and services use their personal data, particularly when data is re-used. For this, it is important that consumers are not confronted with a flood of technical explanations, but they need meaningful information to truly understand the consequences of ADM. Transparency around data use is also key for consumers to be able to exercise their rights under the GDPR (e.g. right to object, erasure, access, etc.).

When it comes to the use of sensitive data which are processed for scientific research or for reasons of public interest, the level of protection is lowered. For example, health data might be taken retrospectively from the disease registry, biobank or from electronic health records without the patient's knowledge. Since in all those cases consumers still have to be adequately informed when the data is collected, a clear and AI specific ethical standard framework is needed to avoid data misuse.

[8] Articles 12-14 GDPR.

The right to explanation of automated decisions

Under the GDPR, consumers have the right not to be subject to a decision based solely on automated processing which produces legal effects concerning him or her or similarly significantly affects him or her (Article 22 of the GDPR). However, this does not apply if the decision is necessary for entering into, or for the performance of a contract. It also does not apply if the decision is based on the data subject's explicit consent.

In such cases, users have at least the right to obtain human intervention on the part of the controller, express his or her point of view, and to contest the decision. One of the key questions that arises from the transparency obligations around automated decision making and the right to contest an automated decision that are comprised in the GDPR is whether a consumer has the right to request an explanation of a decision, in other words an explanation of how the machine has arrived at its result, as this is supported by Recital 71 of the GDPR.

It is therefore important to broadly interpret the GDPR to ensure that users can effectively exercise the right to contest an automated decision[9]. Consumers must be able to understand how AI powered decisions that affect them, such as the assignment of a credit score or creditworthiness check, are reached and therefore be able to exercise their rights to contest the decisions if necessary.

GDPR Accountability

Embedded into the GDPR, the accountability principle requires companies to demonstrate that they comply with data protection rules. Controllers must implement appropriate technical measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation. Those measures must be reviewed and updated where necessary.

Companies will be held liable for the misuse of personal data unless they can demonstrate that they were not in any way responsible for the event giving rise to the damage (Article 82 GDPR). Hence, companies must always be able to demonstrate that their use of data is in compliance with EU data protection rules. The question arises how companies can demonstrate that their AI technology is complying with the rules, especially when machines become autonomous and learn by themselves.

In terms of assigning responsibility when data has been processed unlawfully, it is necessary to assess if and to what extent a company relying on AI could potentially be exempted from the GDPR, and if so, under which circumstances. Guidance from Data Protection Authorities on this point would be helpful. We must ensure that any existing or potential legal vacuums are identified and thoroughly addressed.

[9] However, interpretation varies on this point and the conclusion of some academic analysis is that such a right to explanation is not granted under the GDPR; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469.

Policy recommendations:

- Artificial Intelligence must be developed and used in full respect of EU data protection rules, considering in particular the principles of fairness, transparency, purpose limitation, data minimisation, accountability and privacy by design.

- AI technology should integrate effective mechanisms for consumers to stay in control of their data and exercise their data protection rights, in particular their right to receive meaningful information about the logic and consequences of automated decisions (Articles 14-15 GDPR) and their right not to be subject to decisions based solely on automated decision making (Article 22 GDPR).

- The European Data Protection Board (EDPB) should develop specific guidance regarding the application of the General Data Protection Regulation in the context of Artificial Intelligence. A clear indication of whether the GDPR entails the right to an explanation of an automated decision is particularly necessary. If the conclusion is that it is not the case, such a right should be established in law.

- Data protection authorities and consumer protection agencies should work together to face the problem of information asymmetry and fairness of contractual clauses that provide the rights and obligations of the consumer vis-à-vis the supplier of the AI-based service.

7. Algorithmic accountability and ADM audit

Besides the GDPR, which deals with the processing of personal data, the question arises how to approach algorithmic accountability in general, including situations where non-personal data are processed or where personal data are processed but the GDPR does not apply.

As demonstrated earlier, associated risks to ADM, such as discrimination or lack of informed decision may certainly also occur outside of the realm of data protection laws. An important question is how to ensure proper auditing of algorithms and who can be held responsible in case of consumer harm.

It should be a general principle that companies must introduce effective mechanisms for auditing AI's use of data. For example, bias could be built into an algorithm, but it could also develop as an unintended consequence of an automated self-learning process. Algorithmic auditing could become in the future as important, necessary and common as financial auditing. To ensure that it is carried out with the required independence and adequate technical skills, the possibility of creating effective control systems should be considered. For example, specific organisations, public bodies or departments could be in charge of algorithmic auditing.[10] A measure of last resort could be the prohibition of certain ADM processes.

[10] Control could be carried out using a layered approach. For example, a public institutions issues certificates, an independent but publicly legitimised body checks ADMs and publishes peer reviews, or a company employee acts as a certified controller for algorithmic accountability (similar to the established company internal controllers for data protection).

7.1. Which ADM processes are to be audited? Relevance criteria and legal compliance

It should be discussed whether all ADM processes should be up for control or only those which are socially most relevant, or which are inclined to produce the associated risks discussed above. A starting point for relevance could be the significance of the process to society, including the significance of the legal affects concerning individuals (in line with the GDPR rationale). It will be necessary to develop relevance criteria, which takes into account the social-economic dimension of algorithms and the dependency of users who rely on them.

As a principle, auditing should always be possible to assess whether legal obligations under the data protection rules, EU consumer law, or sector-specific rules are upheld and whether non-discrimination is ensured. It must also be ensured that qualified entities are empowered and financially equipped to perform the necessary investigations and to take the appropriate measures to stop identified infringements of law.

It should also be considered how the general public, hence the persons potentially affected by ADM processes can access information about ADM processes. This could be done by granting a right to information and establishing a duty of companies to disclose the relevant processes for a decision upon request without disclosing the programming code or any other IP or trade secrets.

7.2. To what extent and at which point in time?

A related question is to which extent details of (the functioning of) algorithms or other parts of the ADM processes must be published in order to ensure a proper auditing without compromising protected trade secrets. Technical standards and the realisation of an accountability by design/ethic by design principle would be helpful. For example, an "audit trail" could help to comprehend on which level a decision was taken that led to a harmful event. It must also be discussed at which point in time a control or auditing of ADM processes should take place. This may well depend on the ADM process in question and for which purpose it was used.

7.3. Appropriate Measures

Once the relevance has been established and auditing has been carried out, a decision must be taken about how to react to the result of the investigation. For this purpose, it will be necessary to establish criteria based on which the appropriate measures can be chosen. Those measures could exclude transparency obligations, adaption of the ADM processes to comply with the law, or – as a last resort measure – the prohibition of (parts of) the ADM process for a certain purpose.

Policy recommendations:

- It should be a general principle that companies must introduce effective mechanisms for auditing AI's use of data. ADM auditing should be carried out by independent third parties or specific public bodies. For the question of which ADM processes are up to scrutiny, relevance criteria and standards could be established.

- The general public should have a right to access information about ADM processes and there should be corresponding duties of companies to disclose certain ADM processes.

- Companies developing and using AI technology should invest in innovative ways to inform consumers in a timely and easy to understand manner about the usage of their data, the logic behind it and the consequences that it might entail in order to enable consumers to make informed choices. Education of all players involved in the development and use of algorithmic systems (programmers, business professionals, consumers, etc.) should be fostered.

- It is necessary to establish criteria based upon which the responsible authorities can take the appropriate measures after the ADM audit. Those measures could exclude transparency obligations, adaption of the ADM processes to comply with the law, or – as a last resort measure – the prohibition of (parts of) the ADM process for a certain purpose.

8. Safety and liability

8.1. Safety risks

Greater protection around safety will be vital before consumers can fully embrace the rapid rise of AI and allow machines to play an even greater role in their lives. Among the biggest questions of ADM is the challenge of how to address safety risks and who can be held liable in case of consumer harm.

For example, advanced robots or IoT products may malfunction or act in a way which was not foreseen at the time at 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. Public authorities, as well as producers, must minimise potential risks to consumers that are caused by a product which is brought to the market.

The EU safety framework, for example the Machinery Directive or the General Product Safety Directive already address the intended use and foreseeable misuse of products. However, there is no specific safety standard in place that relates to products with embedded software, whose functions are based on automated decision making.

8.2. Liability

The standard of safety is also the basis of current EU liability rules. Product liability follows the rationale that the one who makes a profit from dangerous activities should be held accountable. There should be a fair allocation of responsibility for risks.

However, the relevant EU Directive dates from 1985 and is not up to date regarding problems created by technological advancements, including automated and autonomous products, cloud technology, or robotics.

For example, product liability follows the traditional understanding that only the producer of a manufactured tangible product can be held responsible. Such an understanding is inappropriate when it comes to, for example, the Internet of Things.

As a principle, the Directive should also apply to any professional in the product supply chain, including creators of digital content or software, when his activities have affected the safety of a product which was then placed on the market. Then, there is a problem about how to identify the liable person when the same product is made by several producers and contributors. There should be joint liability of professionals in the product supply chain. Since the consumer has the onus of burden of proof, the victim will have otherwise no possibility of recourse under the current Directive.

It is therefore disappointing to see that the European Commission, in its recently published Communication on Artificial Intelligence[11], does not recognise the urgency of reforming the Product Liability Directive to achieve these important objectives, etc.

8.3. Digital products are also products

Another problem is the scope of the current rules on liability, which were developed in view of manufactured movable goods rather than of digital products, such as software. It is clear that the rules on liability do not govern defective digital services at all. It is time to consider digital content products a product under the Product Liability Directive whereas making them available, for example on a tangible data carrier or the internet, should be considered as bringing the product into circulation. Also, the concept of damage is not fit for practice as it does not cover damage to the digital environment or consequential harm that results from AMD processes.

8.4. Development risk-defence

It is also unclear how the exceptions for liability apply to AMD based products. Under current rules, the producer is exonerated from liability if the state of scientific or technical knowledge did not allow him to detect the defect at the moment where the product was brought into circulation. Yet, what is the 'state of scientific and technical knowledge' when it comes to smart products or applications?

All those questions need to be addressed. There is an urgent need for a policy debate on whether the EU law maker should not better abandon the concept of "defect" in favour of a real "strict liability" system, which focuses on safety risks and hazards. The focus should be whether safety risks materialise, and consumers are harmed, despite having correctly used the product as agreed and expected. If so, professionals in the supply chain should be held responsible for the damage or harm occurred.

[11] Artificial Intelligence for Europe - COM(2018) 237 final.

Policy recommendations:

- EU law makers should work on a specific legal standard for safety that relates to products with embedded software, particularly where they use algorithmic decision making. For this purpose, it should be analysed whether the EU safety framework is fit for practice, in particular the General Product Safety Directive. New rules should obligate traders to implement a safety and security by design and by default principle.

- Market surveillance mechanisms should be fit for practice and able to ensure that unsafe or potentially insecure products do not reach the market or will be immediately taken off the market when a hazard can be assumed or has already been identified. It will be important to ensure that market surveillance authorities and consumer authorities are adequately equipped with money and know-how to lead the necessary investigations. EU law makers should work to ensure cooperation of authorities within and without the European Union and develop strategies to cope with risks associated to ADM processes outside of the Union which harm cause damage to consumers within the Union.

- The European Commission should adopt modern liability rules for situations where consumers are harmed by unsafe or defective products, digital content products, and services. It should address risks that arise from modern technologies, including robotics, Internet of Things, and AMD. The focus should be on safety risks and hazards rather than on what constitutes a "defect".

- As a principle, any professional in the product supply chain, including creators of digital content or software, should be held responsible for consumer harm or damage if their activities have affected the safety of a product which was then placed on the market.

- Digital content products should be considered a product under the Product Liability Directive. Making those products available should be considered as bringing the product into circulation.

- The concept of damage should be redesigned to cover damage to the digital environment and consequential harm that results from AMD processes. The first was already considered in the Commission's Proposal for a directive on certain aspects concerning contract for the supply of digital content[12].

[12] COM(2015) 634 final, Art 14.

BEUC The European Consumer Organisation

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

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