POLICY RECOMMENDATIONS FOR A SAFE AND SECURE USE OF ARTIFICIAL INTELLIGENCE, AUTOMATED DECISION-MAKING, ROBOTICS AND CONNECTED DEVICES IN A MODERN CONSUMER WORLD

European Consumer Consultative Group

Opinion

16. Mai 2018

The European Consumer Consultative Group is the Commission's main forum to consult with national and European consumer organisations.

Since its establishment in 1973, the European Consumer Consultative Group (ECCG) assists the Commission by providing expert advice on EU consumer related issues, issuing opinions and participating in different fora.

It advises and guides the Commission in the creation of policies and activities affecting consumers. It also informs the Commission of developments in consumer policy in EU countries, and acts as a source of information on community action for other national organisations.

This opinion of the ECCG does not reflect the opinion of the Commission nor one of its Services.

More information can be found here: https://ec.europa.eu/info/strategy/consumers/consumer-protection/our-partners-consumer-issues/european-consumer-consultative-group-eccg_en

CONTENT

EXECUTIVE SUMMARY

Machine-learning and automated decision-making in a consumer context

The increasing use of self-learning algorithms and machine-learning that steer processes and take decisions on behalf or instead of humans inevitably leads to a set of societal and ethical questions. From a consumer point of view, Algorithmic Decision Making (ADM), de facto automated decision-making, based on big data, is of particular interest and high importance as the number of affected consumers could potentially be high. As a matter of fact, the ranges for application of ADM in consumers' everyday lives are virtually endless. Artificial intelligence is also no science-fiction of distant future times. Examples include algorithms used by online retailers to tailor prices to individual consumers based on estimates of their location and by self-driving cars to go around.

It is therefore essential that the European regulatory framework of consumer protection is able to meet the challenges posed not only by connected devices but also by automated decision-making. Can we still speak about consumer choice when preferences are defined, predicted, and shaped by algorithms? Consumer organisations call on the European Institutions to assess and revise relevant consumer protection legislation to ensure that consumers rights are respected by algorithms and automated decision making. An elaborated form of accountability and ethical processing is needed to foster the benefits of this use of data but to also address any consequent risks.

Consumer groups therefore call on the European Institutions and member States to ensure the following:

Data protection and privacy

1.1 Consumers' privacy and data protection rights must be properly protected and upheld to address potential harms such as discriminatory practices, invasive marketing, loss of privacy and security breaches.

1.2 Regulators and companies must develop effective means and simple processes for consumers to exercise their 'right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her' (Art. 22 GDPR). Only then can consumers effectively challenge outcomes of automated decision-making.

Transparency and public control

2.1 In order to counteract potential negative effects of increased market power and vertical integration in the field of ADM processes and AI policy makers must enable competition authorities to more effectively take into account sources of market power relevant to AI and data driven markets. In evaluating the abuse of market power or the effects of mergers and acquisitions, data or AI systems of the merging parties should be taken more into account, as they could be used to leverage market power from one market to another. The European Commission should consider introducing a new criteria in the jurisdictional rules of the EU Merger Regulation.

2.2 It should be clear to consumers if socially relevant ADM-processes make decisions about them that affect the quality, price or access to a service.

2.3 The appropriate supervisory authorities should ensure the proper enforcement of articles 13, 14, 15 and 22 GDPR and ensure the use of algorithms is lawful and does not take socially unwanted detrimental decisions based on information about consumers. Regulators or another controlling institution should consider appropriate frameworks to address *problems should they arise which should include duties for transparency, rights to information and rights to challenge automated decisions based on personal and non-personal data that produce legal effects. Regulators or another controlling institution should have the right to access and check socially relevant algorithmic decision-making applications. The criteria for identifying such relevant processes must be developed.*

2.4 Some algorithmic decision-making processes must be made transparent to the public to secure free consumer decisions in future and have an informed debate about opportunities, risks and challenges of algorithmic decision-making. Consumers must be given transparency on the logic behind relevant ADM processes, which includes transparency on the data upon which a decision is based and the criteria behind the decision. ADM processes must be made available to peer-to-peer scientific review. This might require either the disclosure of source code or the use of techniques revealing how an ADM process works without disclosing the source code.

2.5 The data base, the algorithm and other parts of the ADM processes muss be designed in a way as to comply with legal obligations. In order to achieve that, rules and standards for compliant machine-learning applications must be developed. These rules must comprise standards for accountability-by-design to enable an external control or audit of ADM processes. Should legal obligations be infringed, the legal framework must provide for tools to oblige providers to alter the algorithm or ban it altogether.

2.6 Public authorities and/or qualified entities must be put in charge to control algorithmic system design and function. Competition regulators should have the power to investigate the links between the use of artificial intelligence, machine-learning or ADM, automated price setting (algorithms)[1] and advertising revenues to be able to detect anti-competitive behaviour and carry out sector- or company-specific investigations.

2.7 Consumers must have the right to access and a re-check by a qualified person of an automated-decision even when the process is not based on personal data. Consumers must also have the right to be heard, to receive a justification for the decision and contest the decision to correct an inappropriate decision.

2.8 There must be financial support available for research activities to develop 'discrimination-aware data processing' and 'fair machine-learning' to prevent unfair decision-making.

Security, safety and liability

3.1 European safety legislation, first and foremost the Safety and the Product Liability Directives, needs to be reviewed to reflect technological developments. The definitions of 'damage' and 'defect' need to be altered to reflect the complexities of embedded self-learning algorithmic decision-making software in tangible goods as well as to address the problem of harm that might be independent of the presence of a defect as currently defined.

3.2 A clear and robust product liability framework that protects consumers if they suffer a damage caused by unsafe connected products or services is essential. The lack of transparency of automated decision-making, especially when based on machine-learning applications, and the enormous complexity of those processes must not mean that consumers have to shoulder potential damages. As new risks arise, liability rules governing

[1] On the problem of collusion by pricing algorithms in eCommerce see Antonio Capobianco and Pedro Gonzaga (2017): "Algorithms And Competition: Friends Or Foes?", Competition Policy International, 14th August, 2017 https://www.competitionpolicyinternational.com/algorithms-and-competition-friends-or-foes, last viewed on 21st March 2018

the safety and liability standards should be introduced, replaced or updated, where necessary. The burden of proof should not be on the consumer.

3.3 The European law-makers should consider the introduction of a 'strict liability' framework in the EU. The framework must ensure consumers must be fully compensated in case they are harmed.

*3.4 The exemptions linked to '*development risks defence' *need to be reviewed in order to minimise dangers stemming from 'smart' products and applications.*

3.5 Consumers should not bear the risk of new advances in internet of things technology, market surveillance mechanisms should be fit for purpose and able to ensure that unsafe or potentially insecure connected products do not reach the market or will be immediately taken off the market when a hazard is identified.

3.6 Companies should adopt best practice standards such as security by design and by default, and be subject to independent assessments of compliance. In case of security incidents or data breaches, they must be subject to timely and adequate notification obligations, liability and compensation rules, and sanctions in case of neglect.

3.8 Liability rules should cover all types of products, digital content products, and (digital and other) services that comprise the internet of things ecosystem.

3.9 Rights to redress for internet of things products and services should not be less than those available for other forms of commerce. Complaints handling and redress mechanisms should be accessible, affordable, independent, fair, accountable, timely and efficient.

3.10 Aggregate information with respect to complaints and their resolutions should be made public.

Research and the role of consumer organisation

4.1 The European Commission must commission extensive research and make available funding to foster understanding of the existing and applicable legal framework for 'artificial intelligence', its gaps, how to fill them, as well as to explore the understanding, attitudes, acceptance and expectations of consumers when it comes to automated decision-making processes and artificial intelligence applications. This research should include consumer surveys and in-depth research based on focus group interviews.

4.2 Via dedicated funding, consumer organisations should be supported in their task to assess the safety and security of applications and bring it to the attention of the public.

A. What is ‘artificial intelligence’?

According to Poole, Mackworth & Goebel (1998)[2], ‘computational intelligence’ “is the study of the design of intelligent agents. An agent is something that acts in an environment—it does something. […] An intelligent agent is a system that acts intelligently: **What it does is appropriate for its circumstances and its goal, it is flexible to changing environments and changing goals, it learns from experience, and it makes appropriate choices given perceptual limitations and finite computation** [highlights added].”In more basic terms and according to participants in the OECD’s Technological Foresight Forum 2016[3], “Artificial Intelligence (AI) [i]s the capability of a computer programme to perform functions usually associated with intelligence in human beings, such as learning, understanding, reasoning and interacting, in other words to "do the right thing at the right time". For example, machines understanding human speech, competing in strategic game systems, driving cars autonomously or interpreting complex data are currently considered to be AI applications.”

A more useful and less nebulous way to qualify what is actually happening would be ‘machine-learning’, a terminology already coined in 1959. Colloquially, this is referred to as giving computers the ability to learn without being explicitly programmed[4].

In order for computer code (the algorithm) to evolve (‘learn’), it needs to be exposed to large data sets to ultimately be able to process unknown sets of data and make predictions on that basis. Depending on the complexity of the task or the pattern, large data sets are required to train the algorithm. These data sets are usually referred to as training data. The training data and the data finally analysed could be ‘big data’ – a *volume* of data that is very large, so that patterns can emerge while it is being analysed, whose analysis is so *quick* that it can happen in real-time, the *origins* of which are extremely diverse and whose *analytics* is being used to make predictions (based on data from the past). **Machine-learning would not work without massive amounts of data and a high level of computational processing capacity**.

Machine-learning is the key technology that enhances the functionality of products and services and makes them what is often described as ‘smart’. Products and services that were known before now have enhanced functionalities and other devices or services that did not exist previously emerge.

Machine-learning applications can be found in our smartphone and tablet keyboards that recognise our mistyping patterns, it is used in voice-recognition applications such as voice-controlled personal assistants such as Amazon Echo, it slows down our car when we drive to close to the vehicle in front of us, it improves our connected vacuum cleaner robot’s performance or it switches the light on in our house automatically when we are home. **Machine-learning powers the ‘Internet of Things’ (IoT)** and a variety of services and applications (in B2C as well as B2B).

Machine-learning has not only transformed goods, it has also completely transformed services: self-learning algorithms will assess creditworthiness or the suitability of an investment portfolio[5], decide which post of which of our Facebook friends we see at what time, which hotels would match our expectations even before we expressed those, influence

[2] Poole, Mackworth & Goebel (1998): Computational Intelligence: A Logical Approach, p. 1, people.cs.ubc.ca/~poole/ci/ch1.pdf, last viewed on 2nd March 2018

[3] https://www.oecd.org/sti/ieconomy/DSTI-CDEP(2016)17-ENG.pdf

[4] http://ieeexplore.ieee.org/document/5392560/?reload=true

[5] Frankfurter Allgemeine Zeitung: Wenn der Algorithmus das Vermögen verwaltet, 17th August 2016, http://www.faz.net/aktuell/finanzen/fonds-mehr/automatisierte-finanzberatung-wenn-der-algorithmus-das-vermoegen-verwaltet-14384953.html, last viewed on 21st March 2018

decisions on criminal sentences[6], in geographically narrow areas thereby influencing police forces patrols patterns[7], and translate a website in a foreign language into a website with the same design – but in a language we understand.

B. Automated decision-making in a consumer context

The increasing use of self-learning algorithms and machine-learning that steer processes and take decisions on behalf or instead of humans inevitably leads to a set of societal and ethical questions. Algorithmic Decision Making (ADM), de facto automated decision-making, when based on big data, is of particular interest and high importance as the number of affected consumers could potentially be high. As a matter of fact, the range for application of ADM in consumers' everyday lives are virtually endless.

ADM processes include – in our understanding – processes of automated decision making as well as processes where the decision is primarily based on automated processing (e.g. credit scoring, where the final decision formally lies in the hand of a human bank employee). The ADM process is not only comprised of an algorithm but includes among others a range of components such as the collection of training data, the data to be analysed, the setting of (optimisation) goals and selection criteria, the output of the processing and the decision making[8].

In this sense, ADM processes are the broadest form of automated systems that affect consumers. ADM processes include systems ranging from those based on simple rule-based decision making algorithms ("if-this-then-that") to those based on highly sophisticated machine learning like neural networks[9].

Especially the increasing use of self-learning algorithms and machine-learning that steer processes and take decisions on behalf or instead of humans inevitably leads to a set of societal and ethical questions.

Importantly, ADM processes are no science-fiction of distant future times. It is already around us, every day:

Today's cars already dispose of sensors that, in combination with cruise control and road marking recognition keep the vehicle automatically at a specific distance from other vehicles. Similar sensors allow to recognise pedestrians and brake autonomously. Accidents with test vehicles have already demonstrated the challenges in this area[10]. The problems consumers

[6] Angwin, Julia, Lauren Kirchner, Jeff Larson und Surya Mattu (2016): "Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And it's Biased Against Blacks". 23rd May2015 https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing, last viewed on 21st March 2018
Electronic Privacy Information Center EPIC: Algorithms in the Criminal Justice System https://epic.org/algorithmic-transparency/crim-justice/, last viewed on 21st March 2018

[7] See IfmPt Institut für musterbasierte Prognosetechnik Verwaltungs-GmbH (2017): "Near Repeat Prediction", http://www.ifmpt.de/prognostik/ (downloaded on 8th June 2017)
Predictive Policing: Kommissar Computer macht bald hessenweit Jagd auf Einbrecher, Heise Online, 28th July 2017, https://www.heise.de/newsticker/meldung/Predictive-Policing-Kommissar-Computer-macht-bald-hessenweit-Jagd-auf-Einbrecher-3785542.html, last viewed on 2nd March 2018

[8] Katharina Anna Zweig (2016): Working Paper: "Überprüfbarkeit von Algorithmen", https://algorithmwatch.org/de/zweites-arbeitspapier-ueberpruefbarkeit-algorithmen, 26th June 2017, last viewed on 21st March 2018

[9] Artificial neural networks are computing systems vaguely inspired by the biological neural networks that constitute animal brains. Such systems "learn" (i.e. progressively improve performance on) tasks by considering examples, generally without task-specific programming. A well-documented field of application is image recognition.

[10] The State of California Motor Vehicle department lists a total of 59 collisions involving autonomous vehicles since 2014 https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/autonomousveh_ol316+ last viewed on 14th March 2018

can run into are easy to imagine: Mercedes Benz latest S class for example uses Here maps to recognise round abouts and curves. It is one of the few available models on the market that actually decelerates.[11] What if a mistake in the map leads to a driving error (a wrong automated decision) of the semi-autonomous car?

Several companies have developed home assistant systems whose job is to use voice recognition to autonomously perform tasks that consumers would otherwise do when sat at a computer or smartphone. Indeed, millions of consumers already carry autonomous learning assistants in their pockets, wherever they go, as their smartphones contain autonomously learning assistants called Google Assistant or Siri (developed by Apple). Practical testing by the Digital Market Watch project of German consumer association has demonstrated that Google's Home Assistant that is supposed to be activated with the words "OK Google" also awakens when conversations contain "OK Kuchen" – meaning "OK cake" in German – and "OK gut" – meaning "OK, fine"[12]. The unwanted activation of the home assistant system entails that more private conversations are being transmitted and processed by Google than intended. Similar results were obtained for Amazon's Alexa.[13]

The camera Nest Cam IQ produced by Google Nest uses Google algorithms for face recognition in its security camera feature. The face recognition feature is used for 'added-value services' like notifications for the access of known faces or intrusion alarm in case of presence of unknown faces in a room. The information is being processes in a cloud-based system. Facial recognition, however, is equivalent to permanent offline tracking in public spaces. The amount and precision of the data is however far more far-reaching than any online-tracking. Accordingly, the risks linked to data theft are much more serious – they amount to identity theft. Conversely, mistakes in the underlying AI could mean a person does not get access to places it should get access to if the decision is taken automatically. In 2015 for instance, it became known that Google's face recognition software tagged a photo of two Native Americans as 'gorillas'.[14]

Vacuum and lawn mower robots are already giving a hand to a vast number of households, mapping apartment and garden sizes – but can they tell apart a small stick from a cat tail? And how much information does it give to hackers/burglars in case the data leaks?

Companion robots are another area of consumer goods that will see tremendous development over the coming years. They will have access to consumers' most intimate parts of live – access that people often would not grant to their friends. But what if the companion robot that is supposed to check on elderly regularly taking their medication gets it wrong, i.e. because its software learned that the woman's medication was always the one on the right shelf and the man's medication the one on the table and the packages get mixed up? Who controls that the robot instead learns that the woman's medication has a yellow pack and the man's medication is red?

A large part of booking and comparison websites already use dynamic pricing[15]. The variables used to set individual prices remain intransparent for the consumer[16]. Under those

[11] https://www.tomsguide.com/us/connected-car-guide,news-20499.html

[12] Verbraucherzentrale Bundesverband (2018): „Ungewollt gesprächsbereit: Auch Googles Sprachassistent hört mehr, als er soll"; 13th March 2018, https://ssl.marktwaechter.de/digitale-welt/marktbeobachtung/ungewollt-gespraechsbereit-auch-google-assistant-versteht-einiges, last viewed on 14th March 2018

[13] Verbraucherzentrale Bundesverband (2018): „Reaktions-Check: Alexa reagiert nicht nur aufs (Signal)Wort", 20.12.2017, https://ssl.marktwaechter.de/pressemeldung/reaktions-check-alexa-reagiert-nicht-nur-aufs-signalwort, last viewed on 21st March 2018

[14] https://www.forbes.com/sites/mzhang/2015/07/01/google-photos-tags-two-african-americans-as-gorillas-through-facial-recognition-software/#563b2032713d, last viewed 17th May

[15] The Guardian (2017): How much …? The rise of dynamic and personalised pricing, 20th November 2017, https://www.theguardian.com/global/2017/nov/20/dynamic-personalised-pricing, last viewed 21st March 2018.

conditions, from a consumer perspective, price discrimination bears the risk that prices are modelled along criteria that violate anti-discrimination laws (e.g. ethnicity, gender, age, religion, sexual orientation). Today's insurance premiums give a flavour of what that could look like if extended to other goods and services.[17]

And more examples could be listed.

It can be assumed that algorithm-based decisions will increase in future – in numbers and in impact on the way consumers live their lives. It will impact consumers' autonomy and their freedom to take decisions, their choice and how they access products and services. It will profoundly change the way of life of individuals and society as a whole. Those changes might bear chances and risks but they definitely need to be assessed in light of the way they allow or restrict choice, allow or restrict market participation, serve the public interest and reflect the societal values we have enshrined in human and fundamental rights, the European Treaties and national laws. A world of self-learning algorithms raises questions about how decision sovereignty and informational self-determination of consumers can be guaranteed and if and how ADM processes can and are controlled by humans. From a consumer point of view, dealing with algorithmic decision making should pursue the objective to minimise the risks and maximise the benefits so that consumers effectively retain the possibility to take decisions freely, even in a world of self-learning algorithms that can take decisions automatically.

Currently, however, automated decision-making processes are highly intransparent, worse, even those designing them regularly publicly refuse to take responsibility for their output[18]. It remains unclear whether results produced by algorithms are merely correlations or based on real causalities. The result can be arbitrary exclusion, discrimination and increasing inequalities. In a connected world driven by artificial intelligence, the output will be actions taken automatically by machine-learning powered devices such as robots or services based on automated decision processes. Responsibility for those actions, need to be clearly attributed and defined.

[16] To date, *Measuring Price Discrimination and Steering on E-commerce Web Sites* https://www.ftc.gov/system/files/documents/public_comments/2015/09/00011-97593.pdf remains one of the most encompassing empirical studies of dynamic pricing strategies in US eCommerce, demonstrating the opaqueness of the practices. Last viewed on 14th March 2018

[17] It took a ruling of the Court of Justice of the European Union to abolish differentiated pricing between gender in Germany https://www.tagesschau.de/wirtschaft/unisex100.html, last viewed 23rd April 2018.

[18] This article in the New York Times can serve as example https://www.nytimes.com/2018/01/04/opinion/leave-artificial-intelligence.html last viewed on 14th March 2018

C. Potential benefits

Machine-learning powered applications have an enormous potential to bring consumers convenience and time savings. The connected vacuum cleaner robot or the smart plant watering system (both exist already) liberate consumers from household chores – time, that consumers can use otherwise. Machine-learning powered applications can also make devices deliver tailor-made products and services. Applications like speech-to-text and text-to-speech can support people with disabilities and significantly simplify their life (exists already).

Machine-learning applications embedded in goods or simply operating in the background of digital services offer the potential to optimise energy use, take advantage of low prices (the classic argument brought forward in favour of smart energy meters) or easily compare complex offers (price comparison tools). They can potentially increase efficiency and sustainability of devices for instance if they automatically detect that they can go into suspend mode because nobody is home (e.g. smart lighting applications). The application could for instance also self-assess if and when unsafe conditions occur and address them adequately before a negative consequence follows (e.g. the more elaborate version of a 'safety mode' already implemented in boilers).

Machine-learning can also potentially facilitate and improve the work of consumer organisations, research and regulatory authorities: market research might be facilitated and improved in accuracy. Price monitoring can happen in real-time, thus enabling consumers to pick the best deal. Enforcement entities could use self-learning systems to automatically screen unfair contract terms[19] and alert consumers about them before they make an online purchase.

D. Challenges and risks

As the processing of data via the computer code embedded in 'smart devices' or working behind the interface of a digital service is not visible or otherwise tangible for consumers, the biggest concern in relation to machine-learning and IoT devices containing machine-learning applications is the lack of control of the devices by their owners and users and opacity of the decision logic of provided services. This lack of control results in different types of risk and can be grouped into several categories:

1. Data protection and privacy

The concerns relate to the (personal) data that is required to train the algorithm, the (personal) data that is being processed as well as the (personal) data or output that is produced by the algorithm. Who makes sure that the large amounts of data being used to train the algorithm is not biased against certain groups in the population or does not contain illegitimately acquired personal data? Who makes sure that the machine-learning application does not collect and process data in a way that is contrary to the General Data Protection Regulation (Regulation (EU) 2016/679))? And even more: is it useful to focus solely on personal data when consumers can also be classified and possibly be discriminated by sophisticated ADM-processes using non-personal data?

Machine-learning applications that have access to some of the most private parts of consumers' lives should be particularly respectful of consumers' privacy. However, what we see so far is not encouraging:

[19] https://claudette.eui.eu/, last viewed on 23rd April 2018

In 2017, the Federation of German Consumer Organisations (vzbv) analysed the voice-controlled personal assistant ‘Amazon Echo’ and found that the device was recording far more conversation than the user intended as it reacted not only to the activating code word “Alexa” but also to similar words[20]. The same has been found to be true for Google Assistant[21].

Algorithms and decisions based on them are not *per se* more objective than human decisions. Results might be biased, discriminatory or incorrect, for instance if the training data reflects a distorted picture of reality. In that case, the fairness principle of the General Data Protection Regulation (GDPR) would not be met. The Norwegian Data Protection Authority, in its report on “AI and Privacy” writes: “This [fairness] principle requires all processing of personal information to be conducted with respect for the data subject’s interests, and that the data be used in accordance with what he or she might reasonably expect. The principle also requires the data controller to implement measures to prevent the arbitrary discriminatory treatment of individual persons. The Regulation’s preface describes the use of suitable mathematical or statistical procedures as possible measures here.”[22] According to the report, underlying models must comply also with other applicable laws such as non-discrimination based on origin, belief, health status or other.

One of the GDPR’s core principles is the ‘purpose limitation principle’. This requires that the purpose for collecting and using the data must be clearly defined, delimited and stated. Feeding every piece of personal data absorbed by tracking consumers online into algorithms of different sorts and for all kinds of purposes would not be compatible with the purpose limitation principle.

In its AI report, the Norwegian Data Protection Authority also comments on the transparency principle: “Although AI is complex […], the principle of transparent processing of personal data applies with full force in the development and use of artificial intelligence.” Transparency is one of the major tools that will enable consumers’ rights enshrined in article 22 GDPR, namely the right to object to decisions based solely on automated decision-making and producing legal effects or similarly significantly affecting a person. Even if transparency about the process is a necessary precondition for the objection – it is not sufficient. There must be a clear process in place in order for consumers to effectively exercise their right.

Recommendations

1.1 Consumers’ privacy and data protection rights must be properly protected and upheld to address potential harms such as discriminatory practices, invasive marketing, loss of privacy and security breaches.

1.2 Regulators and companies must develop effective means and simple processes for consumers to exercise their ‘right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her’ (Art. 22 GDPR). Only then can consumers effectively challenge outcomes of automated decision-making.

2. Transparency and public control to ensure choice and non-discrimination

Understanding how digital products and services using machine-learning applications work is central for consumers to stay in control of their life as consumers. Due to the black-box

[20] https://ssl.marktwaechter.de/sites/default/files/downloads/kurzbericht_amazon_echo_reaktionscheck_0.pdf
[21] https://ssl.marktwaechter.de/digitale-welt/marktbeobachtung/ungewollt-gespraechsbereit-auch-google-assistant-versteht-einiges
[22] https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf, p. 16.

nature of many applications, it is a relative challenge to get access to clear, concise, meaningful and verifiable information that give consumers clarity and control at the right moment. However, this is also one of the requirements of the GDPR but it is limited to the individual.

Consumer control about machine-learning applications and IoT devices is also restricted by some factors linked to the market. Several characteristics of AI and ADM systems can fuel tendencies of market concentration in AI- and ADM-driven-markets: The development and implementation of specific AI and ADM applications in particular can be subject to economies of scale (e.g. high fix costs of collecting training data and training machine learning applications). Learning effects can benefit large enterprises and early adopters when AI systems improve due to being applied in practise (e.g. the Netflix recommendation and personalisation algorithms improve with the amount of user interactions[23]). Economies of scope can be reaped when AI systems and their training data (e.g. for voice recognition) are employed across markets.

Due to the combination of hardware, software, a good and attached services the risk for vertical integration and – as a consequence – market concentration becomes more and more widespread. As a result, it is easier to lock consumers into a manufacturer's own product(s) or into a closed ecosystem that lacks interoperability or APIs.[24] Consumers risk therefore being faced with less choice and as a result, price increases due to less competition in the market, the inability to use independent providers or repair services or combining different tools and devices according to their choice.

Concentration of market power in AI-driven markets could also result from merger and acquisitions. The Commission currently uses the turnover criterion. It has failed to address corporate reorganisation of companies in online platform markets aiming at buying potential future competitors off the market, e.g. by acquiring companies with high-value assets in the form of Intellectual property rights (data) or the transfer of a client base as they are not immediately translated into a market turnover (e.g. the WhatsApp acquisition by Facebook). Mergers and acquisitions in the field of AI seem to exhibit a similar pattern, being driven by the goal of acquiring technology (intellectual property) and human capital (highly qualified data scientists).[25] The mid-2017 amendment to the German Competition Act is a step in the right direction to address these problems[26].

A lack of competition in the use of algorithms also increases the probability for a biased ADM process to get more and more biased during its application – particularly if an independent algorithm audit is not possible or feasible. Only effective competition can ensure that the most accurate and compliant ADM processes actually are successful.

To protect consumer choice, competition authorities must use the different mechanisms available to identify market failures and act accordingly. Even if the EU rules are still relevant

[23] Ashok Chandrashekar, Fernando Amat, Justin Basilico and Tony Jebara (2017): Artwork Personalization at Netflix, Netflix Technology Blog, Dec 7, 2017, https://medium.com/netflix-techblog/artwork-personalization-c589f074ad76, last viewed on 8th May 2018

[24] Examples are car software controlling the optimisation of the engine or the emission cleaning system, computer and smartphone operating systems.

[25] "In 2017 firms worldwide spent around $21.8 bn on mergers and acquisitions related to AI, according to data provider PitchBook, about 26 times more than in 2015 […]. They are doing this partly to secure talent, which is thin on the ground. Startups without revenue are fetching prices that amount to $5-10m per AI expert." Source: The Economist (2018) 'Non-tech businesses are beginning to use artificial intelligence at scale', Special report "GrAIt expectations", Mar 31st 2018.

[26] Bundeskartellamt (2017): 'Bundeskartellamt - Review of 2017', https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/21_12_2017_Jahresrueckblick.html?nn=3591568, last viewed on 8th May 2018

in data markets where AI and ADM systems are likely to develop, there is a need to update the theories informing competition law enforcement and the design of competition remedies, which should take into account the exclusionary effects of data accumulation and new form of exploitative abuses.

But choice is not only relevant in terms of being able to choose amongst different products. The concept of free consumer choice in a market economy also means that consumers are not being manipulated into taking certain decisions. However, there are more and more examples that suggest exactly that: comparison websites, instead of listing all potentially relevant examples following a consumer's query, preselect the results – sometimes omitting the 'best value for money' offers[27].

Another example that restricts freedom of choice are 'tailored products': According to research of the investigative platform ProPublica, dozens of US employers post job opening ads on Facebook that infringe the Federal Age Discrimination in Employment Act of 1967, which prohibits bias against people 40 or older in hiring or employment.[28] How? They task the Facebook algorithm to show ('tailor') the ad only to Facebook users that the algorithm believes to be between 25 or 36. But what if consumers only have older friends? What if their interests are those of 50-years-olds? What if they fulfil all the criteria to make the algorithm suggest that the consumers are much older than they really are? Algorithmic bias might not only mean that a decision taken about people is wrong or biased – it might also mean that people are excluded from opportunities in the first place. The effects on access to goods and services, the participation in consumption or the inclusion in society as a whole can thus be put at risk for individual consumers and entire consumer groups.

Transparency and accountability for consumers and the wider public

Some machine-learning applications will have a crucial impact on consumers' lives, e.g. 'smart' creditworthiness checks. Can consumers find information about the quality and the choice of data that was used to train the algorithm? Do consumers have a choice of different credit worthiness checks with different levels of quality of their algorithm? Was that data biased? Can consumers check the hypothesis on which an ADM process is based? Can consumers understand how the result was produced, i.e. what the basic logic behind the decision of that ADM process is? What are the criteria for which the algorithm optimises or by which consumers are grouped into categories?

This information should on the one hand enable consumers to understand the implications of ADM processes, especially their use in devices or services using machine-learning (like IoT devices), and most importantly, inform their decision-making. Hence, this information would be required before a consumer enters a contractual agreement, not only when it is subject to data processing. Only the latter part is covered by the GDPR. However, this information needs to be presented and explained in plain language to be of any use for consumers at all.

'Hiding' this crucial information in complicated legal language in terms and conditions, terms of use or other small print cannot qualify as 'plain language and easily accessible' as surveys constantly confirm that terms and conditions are either not being read or not being

[27] CORRECTIV (2016): "Wie das Hotelportal HRS seine Kunden manipuliert", https://correctiv.org/blog/2016/09/21/wie-das-hotelportal-hrs-seine-kunden-manipuliert/, last viewed on 21st March 2018

[28] https://www.propublica.org/article/facebook-ads-age-discrimination-targeting

understood by consumers.[29]. Furthermore, the availability of that type of information could inform the wider public debate and raise awareness.

Transparency and accountability – ADM Audit

On the other hand, transparency is required at an institutional level to ensure systems work in the public interest: it is in the public interest that regulators or a legitimised independent control entity can check whether ADM processes, especially, machine-learning applications comply with legal obligations such as data protection, non-discrimination or rules on specific activities (e.g. financial services advice[30]). It is also in the public interest that, if they do not, supervisory authorities or qualified entities can take appropriate measures according to their powers to stop the infringement, bring sanctions, order redress for harm done and – as an ultimate measure – require the alteration of the application or ban it all together. To uphold the rule of law and make it enforceable, transparency is required. However, to implement such an ADM audit in the public interest does not mean that (all) details of algorithms or other parts of the ADM process, must be published in full.[31] ADM processes could be audited by a trusted institution or group of experts, legally required not to publish an (alleged) trade secret. Information that is essential for the public interest could be published, also in an aggregated form that is easier for consumers to understand. This transparency should not be denied on the basis that algorithms and ADM forms part of trade secrets.

Considering the variety and overwhelming number of ADM processes implemented in practice, an institution controlling or auditing ADM processes must focus on the socially most relevant ADM processes. The criteria for identifying such relevant processes must be developed. The number of consumers affected and the potential detriment for consumers could be first indicators to identify those processes.

It must be discussed whether and how (technical) standards for a principle of “accountability-by-design” could be implemented. These are needed in order to enable a legitimised institution or system to audit or check whether an ADM process is lawful and does not produce socially undesirable detrimental outcomes.[32]

Recommendations

2.1 In order to counteract potential negative effects of increased market power and vertical integration in the field of ADM processes and AI policy makers must enable competition

[29] See for example the representative survey by the Federation of German Consumer Organisations (vzbv) from 2014 www.vzbv.de/cps/rde/xbcr/vzbv/studie-digitalisierung-grafikreport-emnid-2014.pdf or the behavioural study performed by the European Commission https://ec.europa.eu/info/publications/consumers-attitudes-terms-and-conditions-tcs_en

[30] The German “Law on the Prevention of Dangers and Abuse of High Frequency Trading“ (*Gesetz zur Vermeidung von Gefahren und Missbräuchen im Hochfrequenzhandel*) obliges traders to notify the German Financial Services Regulatory Authority that they are engaged in algorithmic trading, document any changes to the system, provide system and risk controls and allow the regulator to audit (inspect and control) algorithms in high frequency trading systems.
https://www.eurexchange.com/blob/496300/cf6ec15ea6eb4c9b1cc093ae8e55e2c2/data/German-HFT-Bill.pdf, last viewed on 2nd March 2018
Federal Financial Supervisory Authority - BaFin (2018): “Algorithmic trading and high-frequency trading”, https://www.bafin.de/EN/Aufsicht/BoersenMaerkte/Hochfrequenzhandel/high_frequency_trading_artikel_en.html, last viewed on 2nd March 2018.

[31] Whether it is useful to publish an algorithm in order to further the understanding of the ADM process is another question. Due to the complexity of some algorithms the answer might be complicated.

[32] “Auditability. The principle of auditability states that algorithms should be developed to enable third parties to probe and review the behavior of an algorithm. Enabling algorithms to be monitored, checked, and criticized would lead to more conscious design and course correction in the event of failure.” Nicholas Diakopoulos and Sorelle Friedler (2016): “How to Hold Algorithms Accountable”, https://www.technologyreview.com/s/602933/how-to-hold-algorithms-accountable/, last viewed on 2nd March 2018

authorities to more effectively take into account sources of market power relevant to AI and data driven markets. In evaluating the abuse of market power or the effects of mergers and acquisitions, data or AI systems of the merging parties should be taken more into account, as they could be used to leverage market power from one market to another. The European Commission should consider introducing a new criteria in the jurisdictional rules of the EU Merger Regulation.

2.2 It should be clear to consumers if socially relevant ADM-processes make decisions about them that affect the quality, price or access to a service.

2.3 The appropriate supervisory authorities should ensure the proper enforcement of articles 13, 14, 15 and 22 GDPR and ensure the use of algorithms is lawful and does not take socially unwanted detrimental decisions based on information about consumers. Regulators or another controlling institution should consider appropriate frameworks to address problems should they arise which should include duties for transparency, rights to information and rights to challenge automated decisions based on personal and non-personal data that produce legal effects. Regulators or another controlling institution should have the right to access and check socially relevant algorithmic decision-making applications. The criteria for identifying such relevant processes must be developed.

2.4 Some algorithmic decision-making processes must be made transparent to the public to secure free consumer decisions in future and have an informed debate about opportunities, risks and challenges of algorithmic decision-making. Consumers must be given transparency on the logic behind relevant ADM processes, which includes transparency on the data upon which a decision is based and the criteria behind the decision. ADM processes must be made available to peer-to-peer scientific review. This might require either the disclosure of source code or the use of techniques revealing how an ADM process works without disclosing the source code.

2.5 The data base, the algorithm and other parts of the ADM processes muss be designed in a way as to comply with legal obligations. In order to achieve that, rules and standards for compliant machine-learning applications must be developed. These rules must comprise standards for accountability-by-design to enable an external control or audit of ADM processes. Should legal obligations be infringed, the legal framework must provide for tools to oblige providers to alter the algorithm or ban it altogether.

2.6 Public authorities and/or qualified entities must be put in charge to control algorithmic system design and function. Competition regulators should have the power to investigate the links between the use of artificial intelligence, machine-learning or ADM, automated price setting (algorithms)[33] *and advertising revenues to be able to detect anti-competitive behaviour and carry out sector- or company-specific investigations.*

2.7 Consumers must have the right to access and a re-check by a qualified person of an automated-decision even when the process is not based on personal data. Consumers must also have the right to be heard, to receive a justification for the decision and contest the decision to correct an inappropriate decision.

2.8 There must be financial support available for research activities to develop 'discrimination-aware data processing' and 'fair machine-learning' to prevent unfair decision-making.

[33] On the problem of collusion by pricing algorithms in eCommerce see Antonio Capobianco and Pedro Gonzaga (2017): "Algorithms And Competition: Friends Or Foes?", Competition Policy International, 14th August, 2017 https://www.competitionpolicyinternational.com/algorithms-and-competition-friends-or-foes, last viewed on 21st March 2018

3. Security, safety and liability

Tragic incidents of the past have led the EU and Member States to adopt a large amount of strict rules to prevent accidents from occurring in future.

As the market moves from mechanic and electronic devices to connected IoT devices with embedded machine-learning applications, safety and security of devices has dramatically decreased[34].

IoT device or application malfunctioning can result from a defect existing when the product was sold or occur at a later stage, e.g. when an update or software patch is being rolled-out at a later stage of use. In case of malfunction, a device or application could act (or react) in an unanticipated and potentially unsafe manner. It could also indirectly lead to a malfunction as software modifications might mean that the device or application cannot work with other technology as require as the update disrupted its ability to do so.

But embedded software also opens up different types of product safety challenges that are not present in not-connected devices: There is an IT security dimension that is new and inherent to IoT devices which, inter alia, opens the door to threats like hacks by wrongdoers. It could imply that the safety of the device is corrupted or that the device's processing capabilities and connections are being used for other forms of harm (mining crypto currencies, launch larger cyberattacks, spy on the consumer and other). But security vulnerabilities can also pose a risk to physical safety in some cases as the US Federal Trade Commission rightly acknowledged in a 2015 report on the internet of things[35]. Connected devices do not only have the potential to distract consumers but consumers could also entirely rely – in error - on the assistance provided by the device or application and injure themselves, third-parties or property as a result. This risk will be significantly higher in some applications as compared to others – robots should be mentioned as category of increased danger to physical safety.

Consumers loose much of their control over goods and services when they deal with machine-learning applications embedded in devices (IoT devices). It must therefore be clear that liability must be established in a different way than traditionally. As stated in the 2016 OECD Recommendation on Consumer Protection in E-Commerce[36] "the appropriate allocation of responsibility for the protection of consumers among relevant e-commerce actors is key to promoting consumer welfare and enhancing consumer trust". However, IoT devices present a particular challenge, namely the fact that current liability regimes distinguish between "hardware" and "software". However, this distinction is no longer useful in IoT devices where some key functionalities of a physical good are delivered by software applications. Enhanced by machine-learning applications, these devices can take, anticipate and predict decisions, without humans intervening.

The liability regime needs to reflect the black-box character and complexity of ADM processes. Since consumers have hardly any insight into ADM processes they cannot adequately recognise – let alone prove – causalities, unlawful contract terms, neglect of duties or fault of the provider of the ADM process. This structural information asymmetry

[34] https://www.stiftung-nv.de/sites/default/files/internet_of_insecure_things.pdf

[35] https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[36] www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf

justifies the adjustment of the current European liability regime towards a system where the burden of proof is shifted more towards the provider [37]

European safety legislation, first and foremost the General Product Safety directive[38] and the Product Liability Directive[39], present the need to be updated: Liability is based on the level of safety a consumer can expect. However, there are no safety standards for IoT products yet, let alone digital services. What is the safety level a consumer can expect from a tangible good with embedded software, whose functions are based on an algorithmic decision making?

Also, liability means liability for a "damage". However, current rules do not take into account damage to the digital environment or consequential harm that results from AMD processes. The follow-on question is "who is responsible for the consumer harm"? Is it the producer of the IoT product or the provider of the software which processes the data which feed into the AMD process? Current rules seem to focus only on the producer of the manufactured product. There are no harmonised rules in place for the accountability of the creators of digital content or software, when their activities have affected the safety of a product which was then placed on the market. If we talk about hubs, providing algorithmic applications or data for ADM processes, there might even be more parties involved. It might present a significant safety risk if that data is inaccurate, corrupted or biased. This risk applies to all sorts of categories of data: personal, non-personal or even so-called metadata.

Another problem is the so-called "development risks defence": A producer of a product is exonerated from liability if he could not have foreseen that the product would not provide the safety a person could expect. It raises serious doubts whether such a liability exemption is justified when it comes to self-learning machines and ADM which process information that are not available at the moment where the products where placed on the market but can have far-reaching consequences.

It should also be analysed whether the concept of "defect" is appropriate at all or whether the better alternative would be to establish a real "strict liability", which focuses on safety risks and hazards without the requirement of a defect. Under such a system, professionals in the product supply chain can be held responsible if safety risks materialise and consumers are harmed who correctly used the product (as agreed and expected).

Linked to IT security issues the implications for liability of this new reality go further: Who is liable if the IoT device turns out to be prone to hacks and results or behaviours of the device are being falsified as a consequence (e.g. consumers are refused a mortgage as a result of a falsified process in a creditworthiness check)? Who is liable if the device or application produces inappropriate or biased results because of incorrect data or incorrect correlations (or spurious relationships) applied by the algorithm?[40] Who is liable if IoT devices or rather

[37] Mario Martini (2017): "Algorithmen als Herausforderung für die Rechtsordnung", Juristen Zeitung (JZ), 1017-1025., pp. 1023 and 1024.

[38] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety

[39] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products

[40] The fintech *Kreditech* analyses data from computers and social media profiles from consumers to calculate a credit rating. The algorithm found that many consumers have a higher risk of defaulting on their credit if they have installed a certain letter font on their computer. It turned out that this font is only used by poker or casino programs. Consumers inclined to gambling may have a higher default risk but a perfectly solvent graphics designer who has installed the font for professional reasons might be denied a credit as a result.
Welt.de (2015): „Gegen Kreditech ist die Schufa ein Schuljunge", 17th April 2015
https://www.welt.de/finanzen/verbraucher/article139671014/Gegen-Kreditech-ist-die-Schufa-ein-Schuljunge.html

their embedded software breaches existing rules such as data protection laws or non-discrimination obligations?

And if consumers were harmed, property damaged or their products and applications do not work as expected – what will be their rights? Who will have the burden to prove the defect, fault, mistake or harm?

Recommendations

3.1 European safety legislation, first and foremost the Safety and the Product Liability Directives, needs to be reviewed to reflect technological developments. The definitions of ‘damage’ and ‘defect’ need to be altered to reflect the complexities of embedded self-learning algorithmic decision-making software in tangible goods as well as to address the problem of harm that might be independent of the presence of a defect as currently defined.

3.2 A clear and robust product liability framework that protects consumers if they suffer a damage caused by unsafe connected products or services is essential. The lack of transparency of automated decision-making, especially when based on machine-learning applications, and the enormous complexity of those processes must not mean that consumers have to shoulder potential damages. As new risks arise, liability rules governing the safety and liability standards should be introduced, replaced or updated, where necessary. The burden of proof should not be on the consumer.

3.3 The European law-makers should consider the introduction of a ‘strict liability’ framework in the EU. The framework must ensure consumers must be fully compensated in case they are harmed.

3.4 The exemptions linked to ‘development risks defence’ *need to be reviewed in order to minimise dangers stemming from ‘smart’ products and applications.*

3.5 Consumers should not bear the risk of new advances in internet of things technology, market surveillance mechanisms should be fit for purpose and able to ensure that unsafe or potentially insecure connected products do not reach the market or will be immediately taken off the market when a hazard is identified.

3.6 Companies should adopt best practice standards such as security by design and by default, and be subject to independent assessments of compliance. In case of security incidents or data breaches, they must be subject to timely and adequate notification obligations, liability and compensation rules, and sanctions in case of neglect.

3.8 Liability rules should cover all types of products, digital content products, and (digital and other) services that comprise the internet of things ecosystem.

3.9 Rights to redress for internet of things products and services should not be less than those available for other forms of commerce. Complaints handling and redress mechanisms should be accessible, affordable, independent, fair, accountable, timely and efficient.

3.10 Aggregate information with respect to complaints and their resolutions should be made public.

E. The role of consumer organisations

Consumer organisations have a long track record of assessing the safety and security of products and services. Just the most recent examples demonstrate that their work is needed more than ever to provide independent research and testing of IoT and machine-learning applications to improve how markets deliver for consumers:

When testing the connected toys Cayla and i-Que, BEUC and ANEC-member the Norwegian Consumer Council discovered that children's voice messages were being transmitted to an American company specialising in voice-recognition and "voice fingerprinting". This voice data is arguably necessary in order to improve and develop the machine-learning system providing the voice recognition, but becomes problematic if the voice data is used for other purposes. Knowing that toys are targeting children, the poor IT security of the toy is prone to manipulation.[41]

In addition to a sound legal framework for AI, it is of upmost importance to secure appropriate and sufficient funding for consumer organisations as unbiased, independent testing and assessment of complex technology is a demanding and expensive task. But it is necessary to keep consumers, the environment and society safe and healthy.

A solid level of funding shall be available for consumer organisations to be able to perform technologically demanding product and service testing in order to uncover flaws or illegitimate uses of ADM process and thus contribute to the public interest. With a direct outreach to more than 4 million individual members and subscribers[42], many more followers, friends and supporters on social networks, millions of European consumers seeking advice and more indirect outreach via press and media work, consumer organisations will play a crucial role in informing the public about opportunities and risks of 'smart' applications. This direct and indirect contact with millions of consumers will be key to help building understanding and trust in artificial intelligence applications, ADM processes and even robot assistants. Research about fears and acceptance of those technologies will be required and consumer organisations are in a unique place to perform that research and inform policy-making. The same goes for consumer information and the education that will be needed in order to build trust in these new applications and services.

Consumer organisations can deliver on those monumental tasks. But they cannot and should not shoulder it on their own. The European Commission must provide for adequate funding of those activities under the different research and policy programmes under the next Multi-annual Financial Framework (MFF). Those funds should explicitly be earmarked to contribute to consumer welfare and the public interest as a whole.

Behavioural insights, findings about the impact on consumer choice (or the lack thereof) and clues about unintended consequences will play a crucial role if machine-learning applications are to be adopted and accepted widely. When the 'collaborative economy' emerged forcefully in Europe, the European Commission's Directorate-General for Justice and Consumer Affairs undertook unprecedented work to analyse the applicable legal framework and its gaps. In the same study, it performed fundamental research, inter alia with focus groups, to get a deeper understanding of consumer behaviour, attitudes and expectations.[43] The same is required to fully reap the benefits of 'artificial intelligence' for consumers and the wider public.

[41] The doll Cayla has been removed on some related grounds in Germany and elsewhere https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2017/17022017_cayla.html

[42] www.beuc.eu/publications/2012-00316-01-e.pdf

[43] http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=77704

Recommendations

4.1 The European Commission must commission extensive research and make available funding to foster understanding of the existing and applicable legal framework for ‘artificial intelligence’, its gaps, how to fill them, as well as to explore the understanding, attitudes, acceptance and expectations of consumers when it comes to automated decision-making processes and artificial intelligence applications. This research should include consumer surveys and in-depth research based on focus group interviews.

4.2 Via dedicated funding, consumer organisations should be supported in their task to assess the safety and security of applications and bring it to the attention of the public.