AK EUROPA

Position Paper
May 2023
Consumers

Digital Fairness

Safeguarding consumer self-determination in the digital world

Executive Summary

Background

The European Commission has launched an initiative (consultation lasting until 20 February 2023) to examine whether EU consumer law ensures "**digital fairness**". In the opinion of the Austrian Federal Chamber of Labour (AK), there is certainly a need for action. The digital economy is gaining more and more power over consumers and citizens through excessive use of data, algorithms and artificial intelligence, while the position of citizens is becoming ever weaker. "Take it or leave it" is often the motto of online providers. Those who go along with that have their behaviour monitored and attempts are made to influence how they act. Consumers are seen as data material and guinea pigs to be manipulated. AK increasingly finds that fair treatment of Internet users is lacking, i.e. there is an absence of transparency, respect and self-determination. As will be shown, this development is perilous not only for consumers, but also for free, democratic societies.

AK Demands

- Digital fairness is unthinkable without **digital sovereignty.** Consumers do not want to be at the mercy of opaque online tactics that undermine their autonomy. Fairness and sovereignty do not arise of their own accord. The imbalance of power and knowledge between the parties involved is too great for that. AK welcomes the indications of adjustments to the existing legal framework (Consumer Rights Directive, Unfair Commercial Practices Directive and Unfair Contract Terms Directive). However, we wish to be clear that massive intervention by the EU legislature is needed to compensate for consumer protection shortcomings in the EU digital package that has been presented or already adopted and to enforce digital fairness as a standard.
- A new approach to consumer protection **is needed in the age of "surveillance capitalism"**. The term was coined by US economist Shoshana Zuboff. It refers to a market economy that uses technical means to siphon off every conceivable piece of personal data from people. It tracks their behaviour in minute detail and analyses and processes it for economic decisions in order to make a profit from behavioural predictions. Thought leaders like Zuboff warn that surveillance capitalism challenges democratic norms.
- **The fitness check of consumer law** offers a unique opportunity to turn powerless consumers (citizens) into self-determined players in a world dominated by digital technologies. The innovation-focused EU digital package – including the Digital Services Act (DSA), Digital Markets Act (DMA), Data Act (DA), Artificial Intelligence Act (AIA), Digital Governance Act (DGA) and the European Health Data Act – must be better counterbalanced by corresponding digital consumer rights. For example, there are no enforceable legal rights to offline use (meaning that core functions of a product do not require an Internet connection). Nor are there enforceable legal rights to general compliance with "Don't Track" statements of intent (when data subjects reject behavioural tracking in general and are tired of using application-based, ineffective cookie management systems). The same applies to tools that make it easy for consumers to control data flows in the case of the Internet of Things and many other examples.

AK's position

Need for action from the point of view of AK

Accordingly, AK expects a digital fairness initiative to strive to safeguard the "**digital human dignity**" of consumers and citizens. The German newspaper FAZ made the following prediction back in 2013: "Consumer protection in the information economy is becoming a politically highly important task. It must develop into an instrument for safeguarding freedom. Ensuring the inviolability of the individual is an entirely new challenge in the digital age. Eric Schmidt [note: former Google executive] writes that personality will be the most valuable raw material of citizens in the future. And identity will exist primarily online. Online experiences will begin even before birth, given that ultrasound photos are already posted online. The consumer in the digital age is becoming a product himself. He is read when he buys, moves, reads, pays, even when he thinks. In the age of big data, potentially everything becomes a market, including social life."

These warnings need to be taken seriously.
The dystopian scenario of consumers who are screened right down to their emotions and thoughts and manipulated, classified, rewarded or sorted according to their behavioural profile must not be allowed to become reality. The data economy must be regulated to provide greater protection for the interests of consumers. The EU digital package fails to do so and has a one-sided focus on innovation and competition. The Commission's consultation questions are indicative of minor legal adjustments with regard to dubious sales methods and contractual arrangements. While expansion of the list of prohibited practices and contract terms is certainly necessary, digital fairness is not limited to solving (pre)contractual problems under civil law, because…

- …**commercial and governmental activities are becoming increasingly interlinked**. For example, the state may wish to evaluate consumer health data generated by smart fitness wristbands pseudonymously for its own purposes (policy direction, healthcare, science). Or, to give another example, government agencies that direct traffic flows may be just as interested in mobility data generated by smart cars as private insurance companies that want to check accident histories. That creates completely new dependencies and consumers lose their overview, their understanding of the scope of the data use and their self-determination.

- …**the EU digital package disregards the interests of consumers**. For example, the Artificial Intelligence Act (AIA) imposes information obligations on AI manufacturers vis-à-vis commercial AI users but does not set out any transparency obligations with regard to consumers affected by AI (with the exception of a labelling obligation for chatbots and emotion recognition). As a further example, the Data Act grants consumers the right to access the operating data of their smart household appliances (in real time), but no right to decide who may or may not use the data, how and for what purpose.

- …**in the digital age, everyone is permanently vulnerable.** Individuals and their behaviour can be tracked online down to the most intimate details. Even prudent data subjects have no knowledge of the processes behind digital interfaces and cannot protect themselves against them (or only with unreasonable effort). With knowledge of a person's lifestyle habits, characteristics and mental state – combined with neurological insights, AI-based predictions and technical interface design – companies can guide and manipulate that person's decisions. Consumers generally have little understanding of the technology they are using, which gives the technology providers a huge advantage.

- …**people's self-determination is at stake**. Traditional marketing techniques also have the potential to exert an influence. However, the classification of a person according to hundreds of personal characteristics – in combination with the latest neuropsychological findings and technical possibilities for shaping behavioural management – are powerful instruments for

undermining the autonomy of "responsible, well-informed" consumers and leading them into situations of digital dependence. The Commission is aware of this potential for abuse. According to the study that it commissioned titled "Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation", the current legal framework is insufficient to protect consumers from having their decisions influenced without their knowledge.

The individual AK concerns about digital fairness

Consumer protection standards need to supplement the rules for AI, IoT, the e-ID, government access to customer data etc.

What does fairness mean in terms of the AIA, Data Governance Act, Data Act etc.? AK believes that it would make sense to have a separate law for digital fairness that is related to the permissions for the digital economy in the EU digital package. What is not desirable is a parallel legal universe for consumer legislation. Consumers would lose out under such a concept. Half a dozen legal acts already provide for de-facto prioritisation of data exploitation over the confidentiality interests of consumers.

AK-Demands:

Regulating competition in the data economy needs to be accompanied by consumer protection that balances interests. Currently, there is a lack of even the most basic principles for digital fairness and self-determination of consumers regarding...

- algorithmic decisions (Article 22 of the GDPR),
- artificial intelligence (Artificial Intelligence Act, AIA),
- liability for AI (AI Liability Directive),
- data flows between public agencies, private companies and data fiduciaries (Data Governance Act),
- data access in the case of the Internet of Things (Data Act),
- the reuse of health data (EU Health Data Space, EHDS),
- confidentiality and privacy in telecommunications and Internet traffic (e-Privacy Regulation),
- proof of identity for consumers (eIDAS, e-wallet (personal digital wallet)).

Market concentration needs to be targeted now, not at a later stage

By then it will be difficult to eliminate. For example, the Commission points to Amazon's worrying dominance on the voice assistant market. Amazon is currently expanding its dominance in the field of smart homes (EU-Commission: Internet of Things for Consumers: EU Commission publishes final report on sector inquiry) and its plans include acquiring a production company for smart robot vacuum cleaners (iRobot). In the case of digital car assistants, closed ecosystems that harm consumer interests are also developing unchecked. As a result, motoring clubs that provide roadside assistance can no longer provide rapid on-site assistance, even for simple battery problems. Vehicles are towed to workshops in a time-consuming and costly manner. That is because of the need for an Internet connection, separate electronic access keys for each type of car and sometimes the exclusive services of an authorised workshop.

AK-Demands:

Closed ecosystems and all the associated financial disadvantages for consumers – as is becoming apparent with smart cars – must be prevented at an early stage through regulation.

Departure from the model of the informed consumer

The assumption that consumers act in a sovereign manner when detailed information is available to them is outdated. Anyone's trust can be easily abused and behaviour can be easily manipulated in the digital economy. We know from our everyday work advising citizens that even extremely well-informed and well-educated individuals transfer their entire fortunes to dubious online investment scammers in the hope of fabulous profits. Consumers are unable to see through complex products or services and the interests of other players in the digital value chain (such as advertising networks). They often cannot make sovereign decisions regarding potential uses and misuses, data protection, default technical settings, interoperability, security requirements etc. AI is capable of exploiting human weaknesses. The AIA fails to acknowledge that reality. Article 5 only prohibits AI systems that exploit the weakness of consumers due to their age, disability or special social or economic situation, and that are likely to cause

psychological or physical harm. If the Commission wants to achieve digital fairness, then it should not be allowed for anyone at all to be manipulated without legal consequences.

AK-Demands:

Manipulation (both subjective intent and objective effect) must be unacceptable and inadmissible per se, regardless of the consumer's individual situation. The model of the permanently vulnerable consumer must replace the model of the average (informed, reasonable, careful etc.) consumer in legislation and case law.

The GDPR is just the beginning

The GDPR has brought improvements (stricter requirements for consent, inclusion of third countries, deterrent sanctions). Overall, however, the legal position of consumers has not improved significantly. The reasons lie in problems with enforcement and, above all, in the shortcomings of the GDPR itself. Meaningless data usage information, unclear default settings, non-transparent algorithmic decisions that are not "exclusively" but "only" partially automated or that are not associated with legal or "significantly" detrimental consequences for consumers and unlimited or long storage periods, with data protection authorities being completely inconsistent in their assessment of what the "necessary" storage period is. Declarations of consent are rare, as companies rely on vague permissions such as "overriding legitimate processing interests", "contractually agreed or legally allowed algorithmic decision-making," privileges for "statistics, science and research" and a legal basis in AI law for training AI. Digital self-determination is thus largely undermined. The coupling prohibition has proven to be ineffectual. It is entirely unclear when access to online services is not allowed to be made dependent on consent to data use, despite contrived efforts to reconcile data protection demands with "paywalls".

AK-Demands:

Well thought-out solutions have long been on the table. We refer here to the report on relevant experiences and the issues raised by the AK in its position paper on evaluation of the GDPR: Evaluation of the General Data Protection Regulation (GDPR), as well as to the expert opinion commissioned by the Federal Association of Consumer Centres (Evaluation der DSGVO aus Verbrauchersicht, Projektgruppe verfassungsverträgliche Technikgestaltung ("Evaluation of the GDPR from a consumer perspective; project group for constitutional technology design")), Prof. A. Roßnagel, 26 November 2019; (Provet: Evaluation of the General Data Protection Regulation from the Consumer's Perspective).

Fairness by design instead of dark patterns

"Dark patterns" are prohibited to a certain extent under the Unfair Commercial Practices Directive. However, grey areas and legal loopholes make it necessary for the rules to be tightened. Dark patterns refer to psychological online tricks that are used in the design of apps, device menus, platforms, websites etc. to control the behaviour of users. According to the Commission's own surveys (Netzpolitik: European Commission criticises manipulative tricks of online stores), almost all of the online stores surveyed rely on design tricks. What exactly is covered by the term "dark patterns" is unfortunately unclear. The Digital Services Act mentions hard-to-change default settings or deceptive practices designed to push users into transactions. Online platforms must not be designed in such a way that the "autonomy, decision-making and choice" of consumers is impaired.

AK-Demands:

- The practices listed in the cited recital 67 of the DSA should be included in the Unfair Commercial Practices Directive. However, the list may be extended: for example, to include the practice of "confirm-shaming", where language and emotions (e.g., shame or bad conscience) are used to persuade users to make a certain choice or to refrain from doing so.
- For those applying the law, it is important for the grey area between legitimate attempts at persuasion and unjustifiable manipulation techniques to be minimised.
- A new assessment standard for fairness should be introduced, based on the principle of consumers being vulnerable and the introduction of "fairness by design".
- What is perilous is when dark patterns are combined with personalisation practices to exploit individual vulnerabilities. Regulation of dark patterns therefore also means limiting the permissible scope of personalised offers, prices and advertising.
- Manipulation leads not only to financial damage, but also to intangible losses (autonomy, privacy, cognitive strain – for example, if the time spent is patently disproportionate to the information

gained – and psychological impairment). Those affected by dark patterns and manipulative personalisation should therefore be able to claim lump-sum compensation.

- The Artificial Intelligence Act merely requires users to be notified if they are exposed to an emotion recognition system. Individual emotion recognition must be strictly prohibited. See here the opening clause of the GDPR (Article 9(4)), under which even the Member States themselves may introduce or maintain restrictions with regard to the processing of biometric data.

- Incorporation of behavioural findings into the determination of unlawful practices. Authorities can require providers to provide information on behavioural experiments in optimising digital interfaces. The burden of proof for plaintiffs (law enforcement agencies) is eased.

- Revision of the Consumer Rights Directive to make it mandatory to provide a contract cancellation button that makes it as easy to cancel a contract as it is to place an order.

Preserve human dignity

Some of the trends that are currently developing unchecked cannot be reconciled with European fundamental rights at all and instead violate human dignity. The case of the operator of NY Madison Square Gardens, which uses facial recognition to bar lawyers who have filed a lawsuit against it from the venue, illustrates the problems that can result from a lack of prohibitions (Gesichtserkennung im Einsatz gegen unliebsame Anwaltskanzleien - Überwachung (DerStandard: Facial recognition used against disagreeable law firms - Surveillance). PimEyes and Clearview AI are companies that store, biometrically analyse, and catalogue millions of unsolicited facial images from the Internet to build surveillance systems (PimEyes: Loss of anonymity) AI calculates the current emotional states of players for online game providers based on their facial expressions or keystrokes, in order to personalise game characters accordingly, but also to switch to advertising or the next game level at the right moment.

AK-Demands:

- Emotion or thought recognition violates personal rights at their core. It is therefore unacceptable that the Artificial Intelligence Act does not contain any consumer protection provisions at all or – with regard to AI-based emotion recognition – only a labelling requirement instead of a ban.

- The use of biometrics must also be strictly limited in consumer transactions to prevent a creeping increase in the requirement for consumers to identify themselves, mass surveillance and the end of anonymity.

Prohibit personalised prices

Behavioural profiling and AI enable real-time tailoring of prices to individual consumers. Thanks to the Modernisation Directive, companies are required to indicate that they use personalised prices. Those affected only know that the price has been tailored to their profile or situation and that there is a risk of disadvantage. The rights of access under Article 22 of the GDPR are of no benefit here: they do not provide meaningful information in advance; instead, they only grant access to information retrospectively and, moreover, often only after time-consuming complaint procedures. Furthermore, that presupposes that the information constitutes personal data (not statistical allocations), that there are legal consequences and that the information does not affect business confidentiality. That means consumers lose their feel for the "normal price" or reference price and instead have a sense of arbitrariness and powerlessness.

AK-Demands:

- Entirely personalised prices should be prohibited.

- In the case of target group-specific prices (minimum group size), consumers need to know the range of possible prices in advance and recognise why they belong to a particular price category.

- Personal data that form the basis for pricing must be limited to a reasonable scope: data requiring special protection under the GDPR must not be used at all.

Artificial intelligence needs to be genuinely trustworthy

Unfortunately, digital fairness looks different: The AI Act (AIA) regulates a few AI applications that are classified as high-risk, including hardly any that are relevant to consumers. Protections are limited still further, with many algorithms that can disadvantage consumers being deemed not "smart" enough to be regulated under the AIA. That approach is entirely wrong because algorithms can also cause enormous harm to consumers (cf. ITA-Studie für Arbeiterkammer: Entmündigung durch Künstliche Intelligenz? ("Institute of Technology Assessment Study for the Chamber of Labour: Disenfranchisement

through Artificial Intelligence?") (oeaw.ac.at) and the Chamber of Labour study on artificial intelligence from a consumer perspective Kuenstliche_Intelligenz_aus_Verbrauchersicht.pdf (arbeiterkammer.at)). Information rights, and thus transparency, are provided only for commercial AI users, but not for consumers and citizens. Legal protection for those affected plays no role in the proposal. Uses that are not classified as "high risk" are probably not allowed to be regulated elsewhere due to full harmonisation. High risk does not translate to a high level of protection. Instead of monitoring by independent authorities, most manufacturers are simply allowed to monitor themselves. "Regulatory sandboxes" turn consumers into guinea pigs. Companies can test AI, under supervision by an authority, before it is ready for the market without having to comply with legislation. Consumers cannot freely decide about their participation: they are neither informed according to the GDPR nor asked for their consent.

AK-Demands:

- Regardless of whether it concerns only an algorithm or actual AI, the AIA must offer protection against everything that is liable to cause damage, irrespective of the technology used.
- Tiered rules for all AI risk classes. Voluntary commitments are inadequate to protect consumer rights.
- A legal entitlement for consumers/citizens to information, traceability, information, autonomy – including to reject AI decisions – and rights of appeal. The GDPR is completely inadequate with respect to governing rights concerning automated individual decisions. Furthermore, the proposal on AI liability does not create the transparency and support for consumers to be able to control AI and sue manufacturers or users.
- Anti-democratic AI systems should be banned instead of patchy bans on only a few forms of social scoring, remote biometric monitoring and behavioural manipulation.
- The risks that manufacturers and users are required to minimise must be specifically identified. They are supposed to reduce threats to safety, health and fundamental rights. However, pecuniary losses and discrimination that does not concern fundamental rights under the ECHR should also not be disregarded. The condition (risk-free or risky) in which AI is allowed to be placed on the market must be specified.
- AI certification must, without exception, be carried out by independent authorities instead of mere self-certification by manufacturers.
- Before AI is ready for the market, experiments in regulatory sandboxes should only be allowed to be carried out if data subjects know about the experiments and give their consent (in cases of high public interest, the approval of data protection authorities may replace individual consent).
- Requirements and prohibitions for the protection of minors should be introduced. We refer to the proposals in the legal opinion of the University of Vienna (Christiane Wendehorst). More on Christiane Wendehorst's findings can be read here: AK: How secure is biometric data and what are the implications for AI regulation?
- Right of consumer associations to bring collective actions.

No social sorting through scoring

We believe this aspect of AI is so important that we have dedicated a separate section to it. Credit scoring to protect loan transactions is only acceptable if the "internal and external sources" that lenders are supposed to use under the Consumer Credit Directive, and scoring methods more generally, are regulated. After all, AI is only as good as the data it uses. There are no rules on the minimum quality and maximum permissible scope of creditworthiness data. As a result, scorings are often unscientific and disadvantageous. In particular, there is a lack of rules on scoring practices applied by credit agencies as the most common source of data. The most extreme form of social scoring is the Chinese social credit system. The AIA does not adequately address this risk. Companies (and public authorities) are not allowed to assess the trustworthiness of individuals on the basis of their characteristics or social behaviour, unless the data were already originally collected for this purpose or the detrimental treatment of an individual or group is not "unjustified" or "disproportionate". In a democratic system, what company or authority can presume to collect personal data in order to numerically assess the trustworthiness and social behaviour of its citizens? Such projects touch upon human dignity, so there is little scope for permissible uses.

AK-Concerns:

- Digital fairness means imposing specific quality standards on credit agencies and scoring managers.
- Social scoring should be banned without exception.

Liability principles for online platforms

Under the Digital Services Act (DSA) , online marketplaces (such as Amazon or the Apple Store) must check third-party details before activating them. The protection is full of holes. Consumers are not able to trust that the information about third-party providers is always correct. The platforms are only required to check third-party products and services for illegality on a random basis using official, freely accessible online databases. There are no liability rules for negligent platforms. This means that there is still a lack of legal certainty as to when platforms must bear liability for errors made by third-party providers. Article 5(3) excludes the consumer protection liability of online marketplaces from the rules for the liability exemptions for host providers. However, that is only the case if consumers are led to believe, based on the manner of presentation by the platform, that the information, goods or services offered originate from the platform itself or from a third-party provider under the platform's authority or control.

AK Demands:

- The DSA governs the cases in which platforms are not liable. There is also a need for liability principles as to when online marketplaces are liable for third-party infringements.
- Consumers should be able to trust that information about third-party providers has been verified and is correct. If the information is incorrect, the platform must be liable. An EU-wide company register assists them in that.
- We refer to the Model Rules of the EU Law Institute (European Law Institute: Model Rules on Online Platforms, Report of the European Law Institute). Accordingly, joint and several liability of the platform provider would apply if the platform violates duties of care or the consumer "may reasonably rely on the platform operator having a predominant influence over the supplier". This requirement is fleshed out by a list of criteria that are missing from the DSA.

Proper customer reviews and self-selected rankings

The Modernisation Directive does not put a stop to falsified customer ratings. Customer ratings still do not have to be verified by the platforms and can be falsified. Platforms only need to provide information as to whether the platform ensures that reviews come from consumers who have actually purchased or used the products and, if so, how it ensures that. It would also represent tangible added value for consumers if they could determine the search criteria for the order of search results themselves: for example, according to the origin of goods or according to meaningful quality labels or environmental labels.

AK-Demands:

- Platforms must finally check the accuracy of entries in their customer rating systems. Minimum measures are: Spot checks and plausibility checks as well as reporting systems for suspicious cases.
- The criteria for the order of rankings should always be up to the users themselves (not only for the "very large online platforms" (VLOPs) under the DSA). In the interest of sustainability, it also needs to be possible to search for the origin of the goods and quality and environmental labels.

Sovereignty instead of dependence in the case of the Internet of Things

The Data Act governing the Internet of Things (IoT) contradicts that principle: all conceivable device data are to be accessible for further use for other purposes. Data subjects are expected to be satisfied with a right of access to the data. Whether and how they can decide on data flows, repairs and resales is left completely open. Two of the many issues that are not resolved with legal certainty are: when are operating data of networked devices deemed personal data and to whom do they "belong"? Consumers run the risk that their right of self-determination over their data or their right of ownership over purchased "smart" products will not be respected. The supply side

- makes use of contractual and technical design options to commercially exploit registration and operating data of the devices,
- assumes little responsibility (assurance of quality, liability in the event of damage, warranty in the event of defects) for risks associated with IoT (software errors, hacking attacks, data breaches, insolvencies of involved providers, damaging use of immature algorithms and AI) and also rarely

invests sufficiently in preventive security,

- weakens consumers since ownership rights to the software associated with a purchase are increasingly being cancelled and replaced by mere rights of use under copyright law.

Car manufacturers see that their revenue from car production is likely to decline and are shifting their efforts towards increasing customer loyalty through smart services based on subscription payments. Apple's commercially successful, closed ecosystem is a prime example. In the worst case, customers will in future be firmly tied to one manufacturer, from the breakdown service through insurance and assistance for (partially) automated driving systems to car maintenance (AK-Study: Interconnected automotive).

Summary of AK concerns

Consumers must still be able to make their own decisions about what to do with the product they have purchased in every respect;

- Own all integrated software components;
- have an unlimited right of self-determination to all data generated by the purchased product;
- be able to decide freely about whether and to whom they make those data available;
- be free to choose their workshops and service providers in every respect; not be forced to accept tie-in contracts (purchase of goods plus maintenance and service contracts or insurance offers that include tracking of product use)
- be confident that the manufacturer or seller will not cite liability or warranty disclaimers if the consumer takes the device to a repair shop of his/her choice or does not make available all the data that has been generated.
- Smart products must have (de)activatable IoT functions and also be usable offline.

Right to offline use instead of being forced to use products online

Consumers want to be able to switch off networked functions (connectivity) and still use the main functions of the product offline. But businesses have other interests (know your customer, more profit through additional networked services, data sales). Thus, the right to be able to deactivate internet connections - without losing core functions of the device - must be legally secured. The importance of this offline right is shown by the insistence of many consumers on a switch-off function for smart meters, digital electricity meters. Many games have to be played online, even when the game is played by one person alone and an internet connection is not required.

AK-Concerns:

Without an offline right that is expressly incorporated, consumers will only have the choice of take it or leave it. Digital sovereignty means being able to use the core functions of a product – as far as technically possible – offline if desired.

Complement the Data Act by consumer rights

The Data Act aims to make data generated by Internet-connected devices available to numerous stakeholders – the users of the products, the "data holder" (manufacturer, seller, lessor or other authorised party), authorised third parties, public bodies and science and research in the public interest. Consumers have the right to be informed about the accumulation of data, to have access to this data themselves (as directly as possible) and to provide third parties with access to the data at their request. But what remains of the user's private sphere when TVs and robot vacuum cleaners are constantly extracting usage data and third parties know exactly when and what the user watches, where and when they are at home, and how big their home is?

AK-Concerns:

- Fairness rules and arbitration bodies are only provided for by the Data Act for the companies involved in the data flow. Consumers (unlike SMEs) do not enjoy any protection (beyond the Unfair Contract Terms Directive) against IoT-specific unfair contract terms. Consumers also need such protections.
- The draft does not address consumer needs and their legal protection interests (with the exception of a right to information, data access and "data sharing"). Consumers who buy products are regarded in the draft as "users" (instead of owners with sole rights of disposal). Ownership of all components of IoT products must be established.
- Consumers do not have a secure right to use their product offline or to restrict data generation. The proposal assumes registration of consumers using IoT devices. That would often be excessive:

no smart car manufacturer needs to know who is currently behind the wheel. It is unclear whether they can resell their individualised product or repair it themselves. These rights of self-determination must be safeguarded.

- It is not clear from the draft who is the so-called data owner amongst several possible parties (manufacturer, additional service provider, software supplier, seller, other third parties). The responsibilities of all players must be regulated in a legally certain manner.

- The Data Act applies equally to personal data and non-personal data. That the provisions do not distinguish between types of data is a flaw. What may be harmless in one case may be a violation of fundamental rights in another. Incidentally, many researchers believe that device data almost always have an (indirect) personal reference that is protected by fundamental rights. To speak indiscriminately of "data" can thus be a calculation: in practice, the data economy will often unreflectively invoke rights of use, which conflicts with the GDPR.

- Public agencies, as well as undefined (and therefore ominous) agencies and entities, may request data if there is an undefined "extraordinary need" to fulfil public interests in an emergency. Digital sovereignty means information rights and consent rights for consumers in such situations. Only in cases of serious public interest (such as a pandemic) can data protection authorities issue general authorisations.

Comprehensive liability for AI

It is not comprehensible that the general Product Liability Directive applies to a large number of products that are likely to have less drastic consequences compared to (high-risk) AI. Nevertheless, this provides for strict liability combined with some simplifications of proof: Under that directive, courts may presume the defectiveness of a product (rebuttable) and/or the causality between defect and damage (rebuttable) if the case is too complex due to the nature of the product, the data or technology used, or causal links that are difficult to prove. If satisfaction cannot be obtained from the party against which the claim is directed, other companies involved in the value chain also bear secondary liability. By contrast, the proposal on AI liability fails to provide victims with swift, affordable and successful means of recovering damages. Do injured parties have the simplest possible access to compensation, given the large imbalance in knowledge between the parties? In AK's opinion, the unsatisfactory answer is: No. The Commission prefers to play for time. Since, according to the proposal, there are no AI products on the market yet that "put at risk important legal rights, such as the right to life, health and property", AI incidents are to be collected over 5 years.

AK-Concerns:

It should not be left until the future to decide whether the introduction of strict liability and/or compulsory insurance is necessary. Digital fairness means providing consumers with the best possible protection through such measures right now. The proposed easing of the burden of proof is so minor and subject to so many conditions that it does not put injured parties in a stronger position. It needs to be significantly improved.

Protection against personalised and manipulative advertising

The DSA prohibits personalised advertising if it is directed at minors. Digital fairness goes further: all consumers have a right to undisturbed privacy. The Electronic Commerce Directive sets out the right to declare all spam as unwanted by entering it in a "Robinson list". That right needs to be updated: a general "Don't Track" statement is in line with the privacy-by-design principle and must be respected by all online players. Cookie management systems relate to individual services and are rejected by most consumers for good reason in view of the time required to change settings. Digital fairness means the provision of simple ways for Internet users to express their desire not to be subjected to profiling and personalised advertising.

AK-Concerns:

Consumers must be able to be active online unobserved, regardless of their age. "Don't Track" must apply universally or be able to be declared in a very straightforward way that is universally applicable to all sites and services. The coupling prohibition of the GDPR (service access may not be made dependent on consent to data processing that is not required) must finally be taken seriously and made more specific. .

Target influencers

Influencers are the stars of social media. Children become their fans from as early as primary school

age and emulate them. Adults tend to underestimate how much influencers mean to children. It is difficult for children to see through the fact that carefully considered business models – based above all on wide-ranging forms of advertising – lie behind the performances of influencers. Even with traditional media such as television, it is not easy for children to recognise advertising or to establish a critical distance from it. The challenge of recognising advertising is even greater for children in the case of influencers, as editorial content can hardly be distinguished from advertising and frequent use is made of product placements. Moreover, influencers are close to the lives of children and their recommendations are perceived like those made by friends.

AK-Concerns:

- Digital fairness means specifying what form highly visible labelling should take for common forms of online advertising.
- An EU monitoring body should systematically monitor influencers in order to ensure the protection of minors as fully as possible.
- A general ban on advertising alcohol and foods that are unhealthy in large quantities should be imposed.
- Easing of the burden of proof must take into account the fact that pecuniary advantages are difficult to prove in the case of surreptitious advertising.
- A strong pushback against currently permissible product placements because it contradicts the principle of separation.
- The Audiovisual Media Services Directive only applies if audiovisual elements predominate in online services. That is misguided, because every electronic media product with text-based, audio-based and image-based elements competes in a similar way for the attention of Internet users. AK has identified 30 different forms of advertising on Facebook alone.
- A new directive could set out general principles for all online media and forms of advertising: for example, the prohibition of disruptive advertising (e.g. popup advertising), advertising with gambling elements (loot boxes in games), exploitation of the urge to play (such as in-app advertising in games) and many more protections.

Biometrics – the human body is not a key for consumer transactions

Just put your finger on the display and your phone is instantly unlocked. Forget about passwords and codes – your finger, your eyes are always with you. Biometric features may seem like a simple solution at first glance, but they are not secure. That opens the floodgates to misuse (AK: Fingerprint, Eyescan & Co). Your fingerprint can't simply be changed like a password after a data theft. Even online photos are problematic, as demonstrated by the Clearview and PimEyes scandals show. When millions of profile pictures were tapped for biometric characteristics. Unfortunately, the Commission is sending worrying signals: the AIA allows remote biometric identification of people in public places under certain conditions. That is a dangerous step towards mass surveillance and far removed from digital fairness.

AK-Demands:

- The uses of biometrics is growing particularly strongly in the consumer sector and – due to the high sales value of the data – this leads to the risk of misappropriation, identity theft and data misuse. Biometrics must therefore not become a business. Trading in biometric data and passing such data on to external third parties should be prohibited as a rule and sanctioned with high penalties.
- Each consumer should be able to decide for themselves whether or not they permit their biometric data to be processed.
- Mandatory check before reaching for biometric data: Before any use of biometric data, data protection authorities should consider whether the processing of biometric data is necessary and appropriate, given the high potential for risk and harm.
- When banking online or unlocking devices, biometric data or their hash values must not be stored.
- Consumers must have the right to choose how they identify themselves.
- Portrait pictures should be classified as sensitive data in order to better protect them from hidden biometric evaluation.
- Facial recognition is a technology that, in today's terms, poses the greatest threat to fundamental rights and democracy. Technical

shortcomings, such as enormously high error rates, technologically exacerbated discrimination, racism, oppression, mass surveillance and loss of privacy, anonymity and personal freedom are reason enough to set tight legal limits.

Electronic identity checks only if absolutely necessary

Companies put in place security measures to protect against fraud and abuse. That increases the pressure on consumers to constantly identify themselves electronically. However, the data needed for verification are a favourite target of identity thieves. Data protection comes up short when consumers have to undergo identity checks even for trivial transactions. However, some methods are particularly risky for consumers, for example, when providers urge users to send an ID copy by email – a highly insecure form of transmission for sensitive data that criminals can easily spy on.

AK-Demands:

- Privacy-friendly rules on when and in what secure form identity checks are allowed. Following the German model, the legislature should allow copies of ID documents only to be produced under certain conditions. In addition, to protect against misuse, every copy of an ID document must be identified as such (for example, with a watermark).

- With the revision of the eIDAS Regulation, the EU is striving for an electronic identity ("e-ID") for all EU citizens. The EU project, which is intended as a model to compete with Apple, Google and others, has met with massive criticism. A permanently assigned identifier for consumers must be firmly rejected. That is because it enables life-long profiling via use of the e-ID in all conceivable commercial and official contacts. Digital fairness means: sector-specific delimitations and generation of new identifiers each time the e-ID is used.

Contact us!

In Vienna:

Daniela Zimmer
T +43 (1) 501 65 12722
daniela.zimmer@akwien.at

In Brussels:

Alice Wagner
T +32 (2) 230 62 54
alice.wagner@akeuropa.eu

Austrian Federal Chamber of Labour
Prinz-Eugen-Straße 20-22
1040 Vienna, Austria
T +43 (0) 1 501 65-0

www.arbeiterkammer.at

AK EUROPA
Permanent Representation of Austria to the EU
Avenue de Cortenbergh 30
1040 Brussels, Belgium
T +32 (0) 2 230 62 54

www.akeuropa.eu

About us

The Austrian Federal Chamber of Labour (AK) is by law representing the interests of about 3.8 million employees and consumers in Austria. It acts for the interests of its members in fields of social-, educational-, economical-, and consumer issues both on the national and on the EU-level in Brussels. Furthermore, the Austrian Federal Chamber of Labour is a part of the Austrian social partnership. The Austrian Federal Chamber of Labour is registered at the EU Transparency Register under the number 23869471911-54.

The main objectives of the 1991 established AK EUROPA Office in Brussels are the representation of AK vis-à-vis the European Institutions and interest groups, the monitoring of EU policies and to transfer relevant Information from Brussels to Austria, as well as to lobby the in Austria developed expertise and positions of the Austrian Federal Chamber of Labour in Brussels.