AK EUROPA

Positionspapier
Mai 2023
Konsument:innen

Digitale Fairness

Selbstbestimmung von Konsument:innen in der digitalen Welt absichern

Zusammenfassung

Zum Hintergrund

Die EU-Kommission prüfte mit ihrer Initiative (Konsultation bis 20.2.2023), ob das EU-Verbraucher:innenrecht „**Digitale Fairness**" gewährleistet. Aus Sicht der Arbeiterkammer (AK) besteht tatsächlich Handlungsbedarf: Die Digitalökonomie gewinnt durch exzessive Datennutzung bzw den Einsatz von Algorithmen und künstlicher Intelligenz immer mehr Macht über Konsument:innen und Bürger:innen, während deren Position zunehmend schwächer wird. „Take it or leave it" lautet häufig das Motto von Onlineanbietern. Wer sich darauf einlässt, dessen Verhalten wird kontrolliert und zu beeinflussen versucht. Konsument:innen sind Datenmaterial und Versuchsobjekte für Manipulationen. Die AK vermisst immer öfter einen fairen Umgang im Sinne von Offenheit, Respekt und Selbstbestimmung gegenüber Internetnutzer:innen. Wie noch zu zeigen ist, ist diese Entwicklung nicht nur für Konsument:innen, sondern auch für eine freie, demokratische Gesellschaften fatal.

AK Forderungen

- Digitale Fairness ist ohne „**digitale Souveränität**" undenkbar. Konsument:innen wollen nicht undurchsichtigen Onlinetaktiken ausgeliefert sein, die ihre Autonomie untergraben. Fairness und Souveränität ergeben sich nicht von allein. Dafür sind die Kräfte- und Wissensungleichgewichte zu groß. Die AK freut sich über sich abzeichnende Rechtsanpassungen im bestehenden Rechtsrahmen (Verbraucher:innenrechte RL, Unlautere Geschäftspraktiken-RL und Missbräuchliche Klauseln-RL). Sie macht aber kein Hehl daraus, dass massive Interventionen des EU-Gesetzgebers nötig sind, um Verbraucher:innenschutzdefizite im vorgelegten bzw schon beschlossenen EU-Digitalpaket auszugleichen und digitale Fairness als Standard durchzusetzen.
- Denn **Verbraucher:innenschutz muss sich im Zeitalter des „Überwachungskapitalismus"** neu orientieren. Der Begriff wurde von der US-Wirtschaftswissenschaftlerin Shoshana Zuboff geprägt. Er bezieht sich auf eine Marktwirtschaft, die mit technischen Mitteln alle nur erdenklichen persönlichen Daten von Menschen abschöpft, ihre Verhaltensweisen bis ins kleinste Detail verfolgt, analysiert und für wirtschaftliche Entscheidungen aufbereitet, um mit Verhaltensprognosen Gewinn zu erwirtschaften. Vordenker:innen wie Zuboff warnen davor, dass der Überwachungskapitalismus demokratische Normen in Frage stellt.
- **Der Fitness-Check des Verbraucher:innenrechts** bietet die einmalige Chance, machtlose Konsument:innen und Bürger:innen in einer von digitalen Technologien beherrschten Welt zu selbstzubestimmten Akteur:innen zu machen. Das auf Innovation ausgerichtete EU-Digitalpaket – bestehend unter anderem aus dem Digital Services Act (DSA), Digital Markets Act (DMA), Data Act (DA), Artificial Intelligence Act (AIA), Digital Governance Act (DGA) und dem European Health Data Space (EHDS) – muss durch korrespondierende digitale Verbraucher:innenrechte besser ausbalanciert werden. So fehlen durchsetzbare Rechtsansprüche auf eine Offline-Nutzung, wenn etwa Kernfunktionen eines Produktes keine Internetverbindung benötigen. Auch gibt es keinen einklagbaren Rechtsanspruch auf die generelle Einhaltung von "Don't-Track"-Willenserklärungen, wenn betroffene Personen beispielweise Verhaltenstracking generell ablehnen und die Verwendung von anwendungsbasierter, ineffektiver Cookie-Management-Systeme nicht entkommen können. Das Gleiche gilt für Werkzeuge, die es den Verbraucher:innen erleichtern, den Datenfluss zu kontrollieren, zB im Fall des Internet der Dinge.

Die Position der AK

Handlungsbedarf aus Sicht der AK

Die AK erwartet von einer Initiative für digitale Fairness Anstrengungen, welche die „**digitale Menschenwürde**“ von Konsument:innen und Bürger:innen sichert. Die deutsche Zeitschrift FAZ prognostizierte schon 2013: „Verbraucherschutz in der Informationsökonomie wird zu einer politisch hochbedeutsamen Aufgabe. Er muss sich zu einem Instrument von Freiheitssicherung entwickeln. Die Unantastbarkeit der Person zu gewährleisten, ist im digitalen Zeitalter eine gänzlich neue Herausforderung”. Eric Schmidt [Anm-,: ehemaliger Google-Vorstand] schreibt: „Persönlichkeit wird künftig der wertvollste Rohstoff der Bürger sein. Und Identität wird vorrangig online existieren. Online-Erfahrungen werden noch vor der Geburt beginnen, wenn schon Ultraschallfotos ins Netz gestellt werden. Der Verbraucher im digitalen Zeitalter wird selbst zum Produkt. Er wird gelesen, wenn er kauft, sich bewegt, liest, bezahlt, sogar wenn er denkt. Im Zeitalter von Big Data wird potenziell alles zum Markt, auch das soziale Leben.“

Diese Mahnungen sind ernst zu nehmen. Das dystopische Szenario von bis zu ihren Emotionen und Gedanken durchleuchteten, manipulierten, klassifizierten, je nach Verhaltensprofil belohnten oder aussortierten Verbraucher:innen darf nicht Wirklichkeit werden. Die Datenökonomie muss mehr im Sinne der Verbraucher:innen reguliert werden. Das EU-Digitalpaket verabsäumt dies und ist einseitig auf Innovation und Wettbewerb ausgerichtet. Die Konsultationsfragen der EU-Kommission deuten auf kleinere Rechtsanpassungen in Bezug auf unseriöse Vertriebsmethoden und Vertragsgestaltungen hin. So notwendig die Erweiterung der Liste verbotener Praktiken und Vertragsklauseln auch ist: Digitale Fairness erschöpft sich nicht in der zivilrechtlichen Lösung (vor)vertraglicher Probleme. Denn…

…**kommerzielles und staatliches Handeln verschränken sich zunehmend.** So kann es sein, dass der Staat Gesundheitsdaten von Verbraucher:innen, die von intelligenten Fitnessarmbändern generiert werden, pseudonymisiert für seine eigenen Zweck (politische Steuerung, Gesundheitswesen, Wissenschaft) auswerten möchte. Ein anderer Aspekt ist, dass staatliche Stellen, welche Verkehrsströme lenken, an Mobilitätsdaten, die von intelligenten Autos generiert werden, ebenso interessiert sein könnten wie private Versicherungsunternehmen, die Unfallhistorien auswerten wollen. Dadurch entstehen völlig neue Abhängigkeiten; wodurch die Verbraucher:innen den Überblick, das Verständnis für den Umfang der Datennutzung und ihre Selbstbestimmung verlieren.

…**das EU-Digitalpaket vergisst auf die Interessen der Konsument:innen:** So sieht das Gesetz über künstliche Intelligenz (KI-Gesetz) zwar Informationspflichten für KI-Hersteller:innen gegenüber gewerblichen KI-Nutzer:innen vor, aber keine Transparenzpflichten gegenüber den von KI betroffenen Verbraucher:innen (mit Ausnahme einer Kennzeichnungspflicht für Chatbots und Emotionserkennung). Als weiteres Beispiel räumt das Datenschutzgesetz den Verbraucher:innen das Recht ein, auf die Betriebsdaten ihrer intelligenten Haushaltsgeräte (in Echtzeit) zuzugreifen, aber kein Recht zu entscheiden, wer die Daten wie und zu welchem Zweck nutzen darf oder nicht.

…**im digitalen Zeitalter ist jede/r permanent verletzlich**: Individuen und ihr Verhalten können online bis zu den intimsten Details getrackt werden. Selbst sorgfältige Betroffene haben von den Vorgängen hinter digitalen Schnittstellen keine Kenntnis und können sich dagegen nicht (oder nur mit unvertretbarem Aufwand) wehren. Mit dem Wissen über die Lebensgewohnheiten, Eigenschaften und den mentalen Zustand einer Person - kombiniert mit neurologischen Erkenntnissen, KI-basierten Vorhersagen und technischem Schnittstellendesign - können Unternehmen die Entscheidungen dieser Person lenken und manipulieren. Die Verbraucher:innen haben in der Regel wenig Verständnis für die von ihnen genutzte Technologie, was den Technologieanbieter:innen einen großen Vorteil verschafft.

…**die Selbstbestimmung der Menschen steht auf dem Spiel**: Beeinflussungspotential weisen zwar auch bereits klassische Marketingtechniken auf.

Die Klassifizierung einer Person nach hunderten persönlichen Merkmalen in Kombination mit immer neuen neuropsychologischen Erkenntnissen und technischen Gestaltungsmöglichkeiten der Verhaltenssteuerung sind aber machtvolle Instrumente, auch die Autonomie „mündiger, gut informierter" Konsument:innen zu untergraben und sie in digitale Abhängigkeiten zu führen. Der EU-Kommission ist dieses Missbrauchspotential bewusst. Der von ihr beauftragten Studie "Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation" zufolge reicht der aktuelle Rechtsrahmen nicht aus, um Konsument:innen vor einer ihnen nicht bewussten Beeinflussung ihrer Entscheidungen zu schützen.

Die einzelnen AK-Anliegen zu digitaler Fairness

Schutznormen für Konsument:innen ergänzen die Regeln für KI, IoT, e-ID, behördliche Zugriffe auf Kundendaten uvm

Was bedeutet Fairness in Bezug auf den AI Act, Data Governance Act, Data Act usw? Die AK hält ein eigenes Gesetz für digitale Fairness für zweckmäßig, das einen Bezug zu den Erlaubnistatbeständen für die Digitalwirtschaft im EU-Digitalpaket herstellt. Was nicht erstrebenswert ist: ein rechtliches Paralleluniversum für die Verbraucher:innengesetzgebung. Verbraucher:innen wären die Verlierer:innen eines solchen Konzeptes. Ein halbes Dutzend Rechtsakte beinhalten de facto bereits den Vorrang für die Datenverwertung gegenüber den Geheimhaltungsinteressen der Verbraucher:innen.

AK-Forderungen:

Flankierend zur Wettbewerbsregulierung der Datenökonomie braucht es einen die Interessen ausgleichenden Verbraucher:innenschutz. Zur Zeit fehlen elementarste Grundsätze für digitale Fairness und Selbstbestimmung der Konsument:innen bezüglich

- algorithmischer Entscheidungen (Art 22 DSGVO),
- Künstlicher Intelligenz (Artificial Intelligence Act, AIA),
- Haftung für KI (KI-Liability Directive),
- Datenflüssen zwischen öffentlichen Stellen, privaten Unternehmen und Datentreuhändern (Data Governance Act),
- Datenzugängen beim Internet der Dinge (Data Act),
- Weiterverwendung von Gesundheitsdaten (EU-Health Data Space, EHDS),
- Vertraulichkeit und Privatsphäre im Telekom- und Internetverkehr (e-Privacy VO),
- Identitätsnachweisen für Konsument:innen (EIDAS, e-Wallet).

Marktkonzentration frühzeitig ins Visier nehmen

Denn später sind sie schwer zu beseitigen. So weist die EU-Kommission bspw auf Amazons besorgniserregende Vormachtstellung bei Sprachassistenten hin. Dieses baut seine Dominanz bei Smart Homes gerade aus (EU-Kommission: Internet der Dinge für Verbraucher: EU-Kommission veröffentlicht Abschlussbericht über Sektoruntersuchung) und plant ua, eine Produktionsfirma für smarte Staubroboter (iRobot) zu übernehmen. Auch bei den digitalen Autoassistenten entwickeln sich unkontrolliert geschlossene Ökosysteme, die den Verbraucheri:nneninteressen schaden. So können Automobilclubs, die Pannenhilfe leisten, selbst bei einfachen Batterieproblemen keine schnelle Hilfe vor Ort mehr leisten. Die Fahrzeuge werden zeit- und kostenaufwändig in die Werkstätten geschleppt. Das liegt daran, dass eine Internetverbindung, separate elektronische Zugangsschlüssel für jeden Fahrzeugtyp und manchmal auch der exklusive Service einer Vertragswerkstatt erforderlich sind.

AK-Forderungen:

Geschlossene Ökosysteme mit allen finanziellen Nachteilen für Verbraucher:innen – wie es sich bei smarten Autos abzeichnet – sind durch Regulierung frühzeitig zu verhindern.

Abkehr vom Leitbild der informierten Verbraucher:innen

Die Annahme, dass Verbraucher:innen souverän handeln, wenn ihnen detaillierte Informationen zugänglich sind, ist überholt. Das Vertrauen von jedem/r kann in der Digitalökonomie leicht missbraucht und Verhalten leicht manipuliert werden. Aus dem Beratungsalltag wissen wir: Auch bestinformierte Akademiker:innen überweisen unseriösen Online-Anlagebetrügern in der Hoffnung auf sagenhafte Gewinne ihr ganzes Vermögen. Konsument:innen durchschauen komplexe

Produkte oder Dienste und die Interessen weiterer Akteure in der digitalen Wertschöpfungskette (wie Werbenetzwerke) nicht. Sie können oft in Bezug auf Anwendungs- und Missbrauchsmöglichkeiten, Datenschutz, technische Voreinstellungen, Interoperabilität, Sicherheitsanforderungen etc keine souveränen Entscheidungen treffen. KI ist in der Lage, menschliche Schwächen nutzbar zu machen. Der AIA anerkennt diese Realität nicht. So verbietet Art 5 nur KI-Systeme, die die Schwäche von Verbraucher:innen aufgrund ihres Alters, ihrer Behinderung oder ihrer speziellen sozialen bzw wirtschaftlichen Situation ausnutzen und dadurch ein psychischer oder körperlicher Schaden wahrscheinlich wird. Will die EU-Kommission „digitale Fairness", dann darf überhaupt niemand ohne rechtliche Konsequenz manipuliert werden.

AK-Forderungen:

Manipulationen (subjektive Absicht wie objektive Wirkung) müssen per se verpönt und unzulässig sein, ganz unabhängig von der individuellen Lage der Verbraucher:innen. Der/die permanent verletzbare Verbraucher:in muss in der Gesetzgebung und Rechtsprechung an die Stelle des Leitbilds des/der durchschnittlich (informierten, verständigen, sorgfältigen usw) Verbrauchers/in treten.

Die DSGVO ist erst der Beginn

Die DSGVO hat Verbesserungen gebracht (strengere Anforderungen an Zustimmungen, Einbeziehung von Drittstaaten, abschreckende Sanktionen). Insgesamt hat sich die Rechtsposition der Konsument:innen aber nicht entscheidend verbessert. Die Gründe dafür liegen einerseits bei der Durchsetzung und vor allem in der Unzulänglichkeit der Datenschutzgrundverordnung selbst. In diesem Kontext sind auch die bedeutungslosen Datenverwendungsinformationen, unklare Voreinstellungen, nicht transparente algorithmische Entscheidungen, die nicht „ausschließlich", sondern „nur" teilweise automatisiert sind zu erwähnen. Meist sind diese Umstände mit rechtlichen oder „erheblich" nachteiligen Folgen für Verbraucher:innen verbunden. Dazu zählen auch unbegrenzte oder lange Speicherfristen, wobei die Datenschutzbehörden völlig uneinheitlich beurteilen, was die „notwendige" Speicherfrist ist. Zustimmungserklärungen sind selten, denn Unternehmen stützen sich auf diffuse Erlaubnistatbestände wie „überwiegende berechtigte Verarbeitungsinteressen", „vertraglich vereinbarte oder gesetzlich vorgesehene algorithmische Entscheidungsfindung", Privilegien für „Statistik, Wissenschaft und Forschung" und eine Rechtgrundlage im KI-Gesetz fürs Trainieren von KI. Digitale Selbstbestimmung wird so weitgehend ausgehöhlt. Das „Koppelungsverbot" wiederum erweist sich als totes Recht. Wann der Zugang zu Onlinediensten nicht von der Zustimmung zur Datennutzung abhängig gemacht werden darf, ist trotz größter Verrenkungen, den Datenschutzanspruch mit „Paywalls" in Einklang zu bringen, völlig unklar.

AK-Forderungen:

Durchdachte Lösungen liegen längst am Tisch. Hierzu verweisen wir auf den Erfahrungsbericht und die Anliegen der AK: Evaluation der Datenschutz-Grundverordnung (DSGVO) sowie auf das Gutachten im Auftrag des Bundesverbands der Verbraucherzentralen (Provet: Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht).

Fairness by Design statt Dark Patterns

„Dark Patterns" sind zwar zum Teil nach der Unlauteren Geschäftspraktiken-RL bereits verboten worden. Grauzonen und Rechtslücken machen aber deren Nachschärfung notwendig. Gemeint sind psychologische Onlinetricks, die beim Design von Apps, Gerätemenüs, Plattformen, Websites uÄ genutzt werden, um das Verhalten von Nutzer:innen zu steuern. Nach eigenen Erhebungen der EU-Kommission (Netzpolitik: EU-Kommission kritisiert manipulative Tricks von Onlineshops) setzen fast alle der untersuchten Onlineshops auf Design-Tricks. Was genau von diesem Begriff umfasst ist, ist leider unklar. Das Digitale Dienste Gesetz erwähnt schwer änderbare Standardeinstellungen oder Täuschungen, um Nutzer:innen zu Transaktionen zu drängen. Onlineplattformen dürfen nicht so gestaltet sein, dass Konsument:innen in ihrer „Autonomie, Entscheidungsfreiheit oder Wahlmöglichkeit beeinträchtigt" werden.

AK-Forderungen:

- Die im zitierten EG 67 des DSA angeführten Praktiken sollten Eingang in die Unlautere Praktiken-RL finden. Die Liste ist allerdings noch auszubauen: zB um die Praxis des "confirm-shaming", bei der Sprache und Emotionen (zB Beschämung, schlechtes Gewissen) genutzt werden, um Nutzer:innen zu einer bestimmten Wahl zu veranlassen oder davon abzulassen.

- Für Rechtsanwender bedeutsam: die Grauzone zwischen legitimen Überzeugungsversuchen und unvertretbaren Manipulationstechniken gering zu halten.

- Neuer Bewertungsmaßstab für die Lauterkeit: grundsätzlich vulnerable Verbraucher:innen und Einführung des Prinzips „Fairness by Design“. Fatal ist, wenn Dark Patterns mit Personalisierungspraktiken kombiniert werden, um individuelle Schwachstellen auszunutzen. Regulierung von Dark Patterns bedeutet daher auch, den zulässigen Umfang personalisierter Angebote, Preise und Werbung zu begrenzen.

- Manipulation führt nicht nur zu finanziellen Schäden, sondern auch zu immateriellen Verlusten (Autonomie, Privatsphäre, kognitiven Belastungen – wenn die aufgewendete Zeit zB im auffälligen Missverhältnis zum Informationsgewinn steht – und psychischen Beeinträchtigungen). Betroffene von Dark Patterns und manipulativer Personalisierung sollten daher pauschale Kompensationszahlungen fordern können.

- Das KI-Gesetz enthält bloße Hinweispflichten auf Emotionserkennung. Individuelle Emotionserkennung muss strikt untersagt sein. Verwiesen wird auf die DSGVO-Öffnungsklausel (Art 9 Abs 4), wonach sogar die Mitgliedstaaten selbst in Bezug auf die Verarbeitung biometrischer Daten Beschränkungen einführen oder aufrechterhalten können.

- Einbeziehung verhaltensbezogener Erkenntnisse in die Feststellung unzulässiger Praktiken. Behörden können von Anbietern Infos über Verhaltensexperimente bei der Optimierung digitaler Schnittstellen verlangen. Kläger (Vollzugsbehörden) erhalten Beweiserleichterungen.

- Überarbeitung der Verbraucherrechte-RL zur verpflichtenden Bereitstellung eines Buttons zur Vertragsauflösung, die eine Vertragskündigung genauso einfach macht wie die Bestellung.

Menschenwürde bewahren

Einige der sich derzeit ungebremst entwickelnden Trends sind mit den europäischen Grundrechten nicht in Einklang zu bringen und verletzen die Menschenwürde. Wohin fehlende Verbote führen, zeigt bspw der Fall des Betreibers des NY Madison Square Gardens, der via Gesichtserkennung Rechtsanwälte vom Veranstaltungsort aussperrt, die gegen ihn prozessiert haben (DerStandard: Gesichtserkennung im Einsatz gegen unliebsame Anwaltskanzleien - Überwachung). PimEyes und Clearview AI sind Unternehmen, die ungefragt Millionen von Gesichtsbildern aus dem Internet speichern, biometrisch auswerten und katalogisieren, um daraus Überwachungssysteme zu bauen (Datenschutz Notizen: PimEyes – Verlust der Anonymität). KI errechnet für Anbieter von Onlinespielen anhand der Mimik bzw des Tastendrucks der Spieler:innen deren momentane Gefühlszustände, um auf dieser Basis Spielfiguren zu personalisieren, aber auch im richtigen Moment zu Werbung oder dem nächsten Spiellevel zu schalten.

AK-Forderungen:

- Emotions- oder Gedankenerkennung verletzen den Kern der Persönlichkeitsrechte. Es ist daher inakzeptabel, dass das KI-Gesetz überhaupt keine Verbraucher:innenschutzvorschriften bzw in Bezug auf KI-basierter Emotionserkennung nur eine Kennzeichnungspflicht statt einem Verbot enthält.

- Auch dem Einsatz von Biometrie sind bei Verbraucher:innengeschäften engste Grenzen zu setzen, um einem schleichenden Identifizierungszwang, einer Massenüberwachung und dem Ende der Anonymität vorzubeugen.

Personalisierte Preise verbieten

Verhaltensprofile und KI machen auf den/die einzelne Verbraucher:in in Echtzeit zugeschnittene Preise möglich. Dank der Modernisierungs-RL haben Unternehmen zwar darauf hinzuweisen, dass sie personalisierte Preise nutzen. Betroffene wissen dann jedoch nur, dass der Preis auf ihr Profil oder ihre Situation zugeschnitten wurde und ein Benachteiligungsrisiko besteht. Die Auskunftsrechte nach Art 22 DSGVO nützen dabei nichts: Sie liefern nicht vorab aussagekräftige Infos, sondern nur nachträglich und überdies oft erst nach zeitaufwändigen Beschwerdeverfahren. Vorausgesetzt werden überdies personenbezogene Daten (nicht statistische Zuordnungen), rechtliche Folgen und dass die Auskünfte keine Geschäftsgeheimnisse berühren. Für Verbraucher:innen bedeutet dies den Verlust des Gefühls für den „Normalpreis“ oder Referenzpreise und den Eindruck von Willkür und ein Gefühl der Ohnmacht.

AK-Forderungen:

- Völlig individualisierte Preise sind zu verbieten.

- Bei zielgruppenspezifischen Preisen (Mindestgruppengröße) müssen Konsument:innen die Bandbreite der möglichen Preise vorab erfahren und erkennen, warum sie einer bestimmten Preiskategorie angehören.

- Personenbezogene Daten, auf welche Preisfestsetzungen basieren, sind auf einen vertretbaren Umfang zu beschränken: Besonders schützenswerte Daten nach der DSGVO dürfen gar nicht verwendet werden.

Künstliche Intelligenz muss vertrauenswürdig sein

Digitale Fairness sieht leider anders aus: Das KI-Gesetz (AIA) regelt wenige, als hochriskant eingestufte KI-Anwendungen, darunter kaum solche, die für Konsument:innen relevant sind. Der Schutz wird noch weiter eingeschränkt: Viele Algorithmen, die Verbraucher:innen benachteiligen können, gelten nach dem AIA als zu wenig „intelligent", um reguliert zu werden. Ein völlig falsches Konzept: denn auch Algorithmen können Verbraucher:innen enormen Schaden zufügen (OEAW: ITA-Studie für Arbeiterkammer: Entmündigung durch Künstliche Intelligenz und AK: Künstliche Intelligenz aus Verbraucher:innensicht). Informationsrechte und folglich Transparenz gibt es nur für kommerzielle KI-Nutzer:innen, nicht aber für Konsument:innen und Bürger:innen. Rechtsschutz für Betroffene spielt im Entwurf keine Rolle. Was nicht als „hochriskant" eingestuft ist, darf aufgrund der Vollharmonisierung auch nicht anderswo reguliert werden. Hohes Risiko bedeutet nicht hohes Schutzniveau: Statt Kontrollen durch unabhängige Behörden dürfen sich die meisten Hersteller einfach selbst prüfen. Sogenannte „Reallabore" machen Konsument:innen zu Versuchskaninchen: Unternehmen können KI beaufsichtigt von einer Behörde vor der Marktreife testen, ohne Rechtsvorschriften beachten zu müssen. Konsument:innen können über ihre Teilnahme nicht frei entscheiden: Sie werden weder entsprechend der DSGVO informiert noch nach ihrer Zustimmung gefragt.

AK-Forderungen:

- Egal ob nur Algorithmus oder schon KI: Der AI Act muss technikunabhängig vor allem Schutz bieten, was schadensgeneigt ist.

- Abgestufte Regeln für alle KI-Risikoklassen. Freiwillige Selbstverpflichtungen sind ungeeignet, um Verbraucherrechte zu schützen.

- Ein Rechtsanspruch für Verbraucher:innen und Bürger:innen auf Informationauskunft, Rückverfolgbarkeit, Autonomie - einschließlich der Möglichkeit, KI-Entscheidungen abzulehnen - und Widerspruchsrechte einzulegen sind zentrale Forderungen der AK. Die DSGVO regelt die Rechte bei automatisierten Einzelentscheidungen völlig unzureichend und auch der Entwurf zu einer KI-Haftung schafft nicht jene Transparenz und Unterstützung für Verbraucher:innen, um KI kontrollieren und Hersteller:innen bzw Nutzer:innen klagen zu können.

- Demokratiefeindliche KI-Systeme sind zu verbieten statt lückenhafter Verbote für nur wenige Formen von Social Scoring, biometrischer Fernüberwachung und Verhaltensmanipulation.

- Die Risiken, die Hersteller und Nutzer minimieren müssen, sind konkret zu benennen. So sollen sie zwar Gefahren für die Sicherheit, Gesundheit und Grundrechte verringern, Vermögensschäden dürfen aber ebenso wenig ausgeblendet werden wie Diskriminierungen, die nicht die EMRK-Grundrechte berühren. Anzuordnen ist, in welchem (risikofreien oder -behafteten) Zustand KI auf den Markt gelangen darf.

- KI-Zertifizierung muss ausnahmslos durch unabhängige Behörden statt bloßer Selbstzertifizierung durch die Hersteller erfolgen.

- In „Reallaboren" darf vor der Marktreife von KI nur herumexperimentiert werden, wenn Betroffene davon wissen und darin einwilligen (bei hohem öffentlichem Interesse kann die Genehmigung von Datenschutzbehörden Einzeleinwilligungen ersetzen).

- Ge- und Verbote zum Schutz von Minderjährigen sind einzuführen, wie es etwas in den Vorschlägen im Rechtsgutachten der Universität Wien dagestellt ist (Christiane Wendehorst). Mehr zu den Erkentnissen von Christiane Wendehorst ist hier zu lesen: AK: Wie sicher sind biometrische Daten und welche Auswirkungen hat das auf die KI-Regulierung?

- Es braucht eine Verbandsklagsbefugnis für Verbraucherverbände

Kein Social Sorting durch Scorings

Dieser Teilaspekt von KI ist uns so wichtig, dass wir ihm einen gesonderten Punkt widmen. Eine Bonitätsbewertung zur Absicherung von Kreditgeschäften ist nur akzeptabel, wenn die „internen und externen Quellen", die Kreditgeber nach der Verbraucherkredit-RL heranziehen und die Scoringmethoden ganz allgemein reguliert werden. Denn KI ist nur so gut wie die von ihr genutzten Daten. Es gibt keine Regeln zur Mindestqualität und zum zulässigen Maximalumfang von

Bonitätsdaten. Entsprechend unwissenschaftlich und benachteiligend sind Scorings oft. Vor allem für Wirtschaftsauskunfteien als häufigste Datenquelle fehlen Ausübungsregeln. Die extremste Form von Social Scoring stellt das chinesische Sozialkreditsystem dar. Der AIA bannt diese Gefahr unzureichend: Unternehmen (und Behörden) dürfen die Vertrauenswürdigkeit von Personen nicht anhand ihrer Eigenschaften oder ihres sozialen Verhaltens bewerten, es sei denn die Daten wurden schon ursprünglich für diesen Zweck gesammelt oder die Schlechterstellung einer Person oder Gruppe ist nicht „ungerechtfertigt" bzw „unverhältnismäßig". Welches Unternehmen oder welche Behörde kann sich in einem demokratischen System anmaßen, personenbezogene Daten zu sammeln, um die Vertrauenswürdigkeit und das Sozialverhalten ihrer Bürger:innen numerisch zu bewerten? Solche Vorhaben berühren die Menschenwürde, weshalb es kaum Spielraum für zulässige Anwendungen gibt.

AK-Forderungen:

- Digitale Fairness bedeutet, dass Wirtschaftsauskunfteien und Scoringverantwortlichen konkrete Qualitätsnormen auferlegt werden.
- Social Scoring ist ausnahmslos zu verbieten.

Haftungsgrundsätze für Onlineplattformen

Nach dem Digitalen Dienste Gesetz (DSA) müssen Onlinemarktplätze (wie Amazon oder Apple Store) Drittanbieterangaben vor der Freischaltung prüfen. Der Schutz ist löchrig. Konsument:innen dürfen nicht darauf vertrauen, dass die Angaben über Drittanbieter auch tatsächlich immer stimmen. Die Plattformen müssen nämlich nur stichprobenartig Produkte und Dienste von Dritten auf Rechtswidrigkeiten anhand von amtlichen, frei zugänglichen Onlinedatenbanken prüfen. Haftungsregeln für sorgfaltswidrige Plattformen gibt es nicht. Damit fehlt weiterhin Rechtssicherheit, wann Plattformen für Fehler von Drittanbietern einstehen müssen. Art 5 Abs 3 nimmt die verbraucherschutzrechtliche Haftung von Onlinemarktplätzen aus den Regeln für die Haftungsbefreiungen von Hostprovidern zwar aus. Dies ist aber nur dann vorgesehen, wenn Verbraucher:innen aufgrund der Plattformpräsentation zur Annahme verleitet werden, dass die angebotenen Informationen, Waren oder Dienste von der Plattform selbst stammen oder von einem Drittanbieter, der von der Plattform kontrolliert wird.

AK-Forderungen:

- Der DSA regelt, wann Plattformen nicht haften. Es braucht auch Haftungsgrundsätze, wann Onlinemarktplätze für Rechtswidrigkeiten von Drittanbietern haften.
- Konsument:innen müssen darauf vertrauen können, dass Angaben zu Drittanbietern geprüft und richtig sind. Sind sie falsch, muss die Plattform haften. Ein EU-weites Firmenbuch hilft ihnen dabei.
- Wir verweisen auf die Model Rules des EU Law Institute (European Law Institute: Model Rules on Online Platforms, Report of the European Law Institute). Danach greift die gesamtschuldnerische Mithaftung des Plattformanbieters, wenn die Plattform Sorgfaltspflichten missachtet oder der/die Konsument:in „vernünftigerweise darauf vertrauen kann, dass der Plattformbetreiber einen beherrschenden Einfluss auf den Anbieter hat". Diese Voraussetzung wird durch eine Liste an Kriterien konkretisiert, die im DSA fehlen.

Richtige Kund:innenbewertungen und selbstgewählte Rankings

Die Modernisierungs-RL schiebt gefälschten Kund:innenbewertungen keinen Riegel vor: Denn Kund:innenbewertungen müssen von den Plattformen noch immer nicht überprüft werden und können gefälscht sein. Plattformen müssen nur darüber informieren, ob und falls ja wie die Plattform sicherstellt, dass Bewertungen von Konsument:innen stammen, die die Produkte tatsächlich erworben oder verwendet haben. Ein spürbarer Mehrwert wäre außerdem für Konsument:innen, wenn sie die Suchkriterien für die Reihenfolge von Suchergebnissen selbst bestimmen können: etwa nach der Herkunft von Waren, nach aussagekräftigen Qualitäts- oder Umweltsiegeln.

AK-Forderungen:

- Plattformen müssen endlich Einträge in ihren Kundenbewertungssysteme auf ihre Richtigkeit prüfen. Mindestmaßnahmen sind: Stichproben und Plausibilitätskontrollen sowie Meldesysteme für Verdachtsfälle.
- Die Kriterien für die Reihenfolge von Rankings sollten die Nutzer:innen immer selbst festlegen können (nicht nur bei den allergrößten Plattformen, den VLOPs, nach dem DSA). Im Sinne der Nachhaltigkeit muss auch nach Herkunft

der Ware und Qualitäts- und Umweltgütezeichen gesucht werden können.

Souveränität statt Abhängigkeit beim Internet der Dinge

Das Daten-Gesetz zur Regulierung des Internets der Dinge (IoT) widerspricht dieser Maxime: Alle nur denkbaren Gerätedaten sollen für die Weiterverwendung für andere Zwecke zugänglich sein. Die Betroffenen sollen sich mit einem Zugangsrecht zu den Daten begnügen. Ob und wie sie über Datenflüsse, Reparaturen, Wiederverkäufe entscheiden können, ist völlig offen. Zwei der vielen nicht rechtssicher geklärten Fragen: Wann weisen Betriebsdaten vernetzter Geräte einen Personenbezug auf und wem „gehören" sie? Konsument:innen laufen Gefahr, dass ihr Selbstbestimmungsrecht über ihre Daten bzw ihr Eigentumsrecht an gekauften „smarten" Produkten nicht respektiert wird. Die Anbieterseite,

- nützt vertragliche und technische Gestaltungsmöglichkeiten, um Registrierungs- und Betriebsdaten der Geräte kommerziell zu verwerten,
- übernimmt wenig Verantwortung (Zusicherung von Qualitäten, Haftung bei Schäden, Gewährleistung bei Defekten) für IoT-immanente Risiken (Softwarefehler, Hackingangriffe, Databreaches, Insolvenzen mitbeteiligter Anbieter, schädigender Einsatz unausgereifter Algorithmen und KI) und investiert auch selten ausreichend in präventive Sicherheit,
- schwächt Konsument:innen dadurch, dass mit einem Kauf verbundene Eigentumsrechte an der Software immer öfter ausgehebelt und durch bloße urheberrechtliche Nutzungsrechte ersetzt werden.

Autohersteller sehen ihre Umsatzerwartungen in der Autoproduktion schwinden und verlegen ihre Anstrengungen auf Kundenbindung durch smarte Services, die auf Abonnementzahlungen beruhen. Das wirtschaftlich erfolgreiche, geschlossene Ökosystem von Apple dient dabei als Vorbild. Im ungünstigsten Fall werden Kund:innen künftig vom Abschleppservice über Versicherungen und den Assistenten für (teil) autonomes Fahren bis hin zur Wartung fix an einen Hersteller gebunden sein (AK-Studie: Vernetzte Automobile).

Zusammenfassung der AK Anliegen

Konsument:innen müssen noch in jeder Hinsicht autonom über das gekaufte Produkt verfügen können;

- Eigentum haben an allen eingebauten Softwarekomponenten;
- ein uneingeschränktes Selbstbestimmungsrecht haben über alle Daten, die das gekaufte Produkt erzeugt;
- ohne jeden Zwang darüber entscheiden können, ob und wem sie diese Daten zugänglich machen;
- ihre Werkstätten und Serviceanbieter in jeder Hinsicht frei wählen dürfen; nicht gezwungen sein, Koppelungsverträge zu akzeptieren (Warenkauf plus Wartungs- und Serviceverträge bzw Versicherungsangebote, die ein Tracking der Produktbenutzung beinhalten);
- darauf vertrauen dürfen, dass der Hersteller oder Verkäufer sich nicht auf Haftungs- und Gewährleistungsausschlüsse berufen kann, wenn der/die Verbraucher:in sich seine/ihre Werkstätte frei aussucht oder nicht alle anfallenden Daten zugänglich macht.
- Smarte Produkte müssen (de-)aktivierbare IoT-Funktionen haben und auch offline nutzbar sein.

Offlinerecht statt Onlinezwang

Konsument:innen wollen vernetzte Funktionen wahlweise abschalten und die Hauptfunktionen des Produktes auch noch offline nutzen können. Unternehmer haben gegenläufige Interessen (Know your Customer, mehr Gewinn durch vernetzte Zusatzservices, Datenverkauf). Somit muss das Recht, Internetverbindungen – ohne Verlust von Kernfunktionen des Gerätes – deaktivieren zu können, rechtlich abgesichert werden. Welchen hohen Stellenwert dieses Offline-Recht hat, zeigt das Beharren vieler Konsument:innen auf einer Abschaltfunktion bei Smart Meter, den digitalen Stromzählern. Bei vielen Spielen besteht Onlinezwang, auch dann, wenn ein Spiel allein gespielt wird und eine Internetverbindung nicht erforderlich wäre.

AK-Anliegen:

Ohne ein explizit verankertes „Offline"- Recht haben Verbraucher:innen nur die Wahl des „take it – or leave it" (akzeptiere oder lehne das Angebot ab). Digitale Souveränität bedeutet, Kernfunktionen eines

Produktes – soweit technisch möglich – bei Bedarf auch offline nutzen zu können.

Dem Data Act Verbraucher:innenrechte zur Seite stellen

Der Data Act zielt darauf ab, Daten, die mit dem Internet verbundene Geräte erzeugen, vielen Beteiligten zugänglich zu machen: den Nutzer:innen der Produkte, dem sogenannten „data holder" (Hersteller, Verkäufer, Vermieter oder sonstigen Berechtigten), berechtigten Dritten, öffentlichen Stellen sowie der Wissenschaft und Forschung im öffentlichen Interesse. Konsument:innen haben das Recht, über den Datenanfall informiert zu werden, auch selbst (möglichst direkten) Zugang zu diesen Daten zu erhalten und Dritten auf ihren Wunsch hin ebenfalls einen Datenzugriff zu verschaffen. Was bleibt aber noch privat, wenn Fernseher und Staubroboter permanent Nutzungsdaten absaugen und Dritte genau wissen, wann bzw was sich X ansieht, wo und wann er/sie daheim ist und wie groß die Wohnung ist?

AK-Anliegen:

- Fairnessregeln und Schlichtungsstellen sieht der Data Act nur für die am Datenfluss beteiligten Unternehmen vor. Konsument:innen genießen (im Gegensatz zu KMUs) keinen (über die Unfaire Klauseln-RL hinausgehenden) Schutz vor IoT-spezifischen, unfairen Vertragsbedingungen. Es braucht auch solche für Konsument:innen.

- Den Verbraucher:innenbedürfnissen und ihren Rechtsschutzinteressen widmet sich der Entwurf (mit Ausnahme eines Rechts auf Information, Datenzugriff und „Daten Teilen") nicht. Konsument:innen, die Produkte kaufen, werden im Entwurf als „user" (statt als Eigentümer mit alleinigen Verfügungsrechten) betrachtet. Das Eigentumsrecht an allen Komponenten von IoT-Produkten ist festzuschreiben.

- Konsument:innen haben kein abgesichertes Recht, ihr Produkt offline nutzen oder die Datengenerierung einschränken zu können. Der Entwurf geht von einer Registrierung IoT-Geräte nutzender Verbraucher:innen aus. Dies wäre häufig überschießend: Kein Hersteller smarter Autos muss wissen, wer gerade am Steuer sitzt. Es ist unklar, ob sie ihr individualisiertes Produkt weiterverkaufen oder selbst reparieren können. Diese Selbstbestimmungsrechte sind abzusichern.

- Wer unter mehreren möglichen Beteiligten (Hersteller, Zusatzdienstanbieter, Softwarelieferanten, Verkäufer, andere Dritte) der sogenannte Dateninhaber ist, geht aus dem Entwurf nicht klar hervor. Die Verantwortung aller Akteure sind rechtssicher zu regeln.

- Der Data Act bezieht sich gleichermaßen auf personenbezogene Daten wie Daten ohne Personenbezug. Dass die Vorschriften nicht zwischen den Datenarten unterscheiden, ist ein Fehler. Was in einem Fall harmlos sein mag, kann im anderen eine Grundrechtsverletzung darstellen. Nicht wenige Wissenschaftler:innen meinen im Übrigen, dass Gerätedaten nahezu immer einen grundrechtlich geschützten (mittelbaren) Personenbezug aufweisen. Unterschiedslos von „Daten" zu reden, kann somit Kalkül sein: die Datenökonomie wird sich in der Praxis oft unreflektiert auf Nutzungsrechte berufen, denen die DSGVO entgegensteht.

- Öffentliche Stellen, aber auch ominöse (weil undefinierte) Agenturen und Einrichtungen, können Daten anfordern, wenn bei der Erfüllung öffentlicher Interessen in einem Notfall ein nicht näher definierter „außerordentlicher Bedarf" besteht. Digitale Souveränität bedeutet Info- und Zustimmungsrechte für Konsument:innen in derartigen Situationen. Nur bei schwerwiegendem öffentlichem Interesse (wie in einer Pandemie) können Datenschutzbehörden Allgemeingenehmigungen erteilen.

Umfassende Haftung für KI

Es ist nicht nachvollziehbar, dass die allgemeine Produkthaftungs-RL für eine Vielzahl an Produkten gilt, die verglichen mit (hochriskanter) KI idR weniger einschneidende Schadensfolgen haben dürften. Dennoch sieht diese eine verschuldensunabhängige Haftung kombiniert mit einigen Beweiserleichterungen vor: Gerichte dürfen die Fehlerhaftigkeit eines Produktes (widerlegbar) und oder die Kausalität zwischen Fehler und Schaden (widerlegbar) vermuten, wenn der Fall aufgrund der Natur des Produktes, der eingesetzten Daten bzw Technik oder schwer zu belegender Kausalitäten zu komplex ist. Sind Anspruchsgegner nicht greifbar, haften subsidiär auch andere an der Wertschöpfungskette beteiligte Unternehmen. Demgegenüber ist der Entwurf für eine KI-Haftung nicht geeignet, Opfern eine rasche, erschwingliche und erfolgreiche Durchsetzung von Schadenersatz zu ermöglichen. Haben Personen, die zu Schaden kommen, einen möglichst niedrigschwelligen Zugang zur Entschädigung

in Anbetracht der großen Wissensasymmetrien zwischen den Beteiligten? Die unbefriedigende Bilanz aus AK-Sicht: Nein. Denn die EU-Kommission setzt lieber auf Zeit: Da noch keine KI-Produkte am Markt seien, die „wichtige Rechtsgüter wie das Recht auf Leben, Gesundheit und Eigentum gefährden könnten", sollen KI-Vorfälle über 5 Jahre hinweg gesammelt werden.

AK-Anliegen:

Ob die Einführung einer verschuldensunabhängigen Haftung und/oder einer Pflichtversicherung erforderlich ist, darf nicht erst künftig entschieden werden. Digitale Fairness bedeutet, Verbraucher:innen schon jetzt durch diese Maßnahmen bestmöglich zu schützen. Die vorgeschlagene Beweiserleichterung ist derart gering und an so viele Bedingungen geknüpft, dass sie die Geschädigten in keine stärkere Position versetzt: und deutlich nachgebessert werden muss.

Schutz vor personalisierter und manipulativer Werbung

Der DSA verbietet personalisierte Werbung, wenn sie sich an Minderjährige richtet. Digitale Fairness geht weiter: Alle Konsument:innen haben ein Anrecht auf eine ungestörte Privatsphäre. Die eCommerce-RL enthält das Recht, durch Eintrag in eine „Robinsonliste" auszudrücken, dass sämtliche Spam-Mails unerwünscht sind. Der Anspruch ist zu aktualisieren: Ein allgemeines „Don't-Track" entspricht dem Privacy-by-Design-Grundsatz und muss von allen Onlineakteuren beachtet werden. Cookie-Management-Systeme beziehen sich auf einzelne Dienste und werden von den meisten Konsument:innen mit Blick auf den Zeitaufwand, Einstellungen zu ändern, aus gutem Grund abgelehnt. Digitale Fairness bedeutet: Einfache Mittel für Internetnutzer:innen, ihren Wunsch, keinem Profiling und personalisierter Werbung ausgesetzt zu sein, ausdrücken zu können.

AK-Anliegen:

Verbraucher:innen müssen sich losgelöst vom Alter unbeobachtet online bewegen können. „Don't Track" muss ganz allgemein gelten bzw auf einfachste und allgemein für alle Seiten und Dienste gültige Weise erklärt werden können. Das Koppelungsverbot der DSGVO (ein Dienstzugang darf nicht von der Zustimmung zu nicht erforderlichen Datenverarbeitungen abhängig gemacht werden) muss endlich ernst genommen und präzisiert werden.

Influencer:innen ins Visier nehmen

Influencer:innen sind die Stars der sozialen Medien. Kinder werden schon im Volksschulalter zu ihren Fans und eifern ihnen nach. Erwachsene unterschätzen tendenziell, wie viel Influencer:innen Kindern bedeuten. Dass hinter den Auftritten wohlüberlegte Geschäftsmodelle stehen, die vor allem auf unterschiedlichsten Werbeformen beruhen, ist für Kinder schwer zu durchschauen. Denn Kindern fällt es schon bei klassischen Medien wie Fernsehen nicht leicht, Werbung zu erkennen bzw eine kritische Distanz dazu aufzubauen. Die Herausforderung, Werbung zu erkennen, ist für Kinder bei Influencer:innen nochmals größer, da redaktionelle Inhalte kaum von Werbung zu unterscheiden sind und Produktplatzierungen häufig vorkommen. Außerdem wirken Influencer:innen nah an der Lebenswelt von Kindern und ihre Empfehlungen werden wie jene von Freund:innen wahrgenommen.

AK-Anliegen:

- Digitale Fairness bedeutet zu präzisieren, wie gut sichtbare Kennzeichnung bei gängigen Onlinewerbeformen auszusehen hat.
- Eine EU-Monitoringstelle sollte Influencer:innen systematisch beobachten, um Jugendschutz möglichst durchgängig sicherzustellen.
- Ein generelles Werbeverbot für Alkohol und in größeren Mengen ungesunde Lebensmittel.
- Beweiserleichterungen müssen dem Umstand Rechnung tragen, dass geldwerte Vorteile bei Schleichwerbung schwer zu belegen sind.
- Ein starkes Zurückdrängen von derzeit zulässiger Produktplatzierung, weil diese dem Trennungsgrundsatz widerspricht.
- Die audiovisuelle Mediendienste-RL gilt nur, wenn bei Onlineangeboten audiovisuelle Elemente überwiegen. Dies ist verfehlt, denn jedes elektronische Medienprodukt mit text-, audio- und bildgestützten Mitteln konkurriert in ähnlicher Weise um die Aufmerksamkeit von Internetnutzer:innen. Die AK hat alleine auf Facebook 30 verschiedene Werbeformen identifiziert.
- Eine neue RL könnte generelle Grundsätze für alle Onlinemedien und Werbeformen enthalten: etwa das Verbot aktionsbehindernder Werbung, Werbung mit Glücksspielelementen (Lootboxen in Spielen), Ausnutzen des Spieltriebes (etwa In-App-Werbung bei Spielen) uvm.

Biometrie - Menschlicher Körper darf kein Schlüssel für Verbraucher:innengeschäfte sein

Finger aufs Display und flugs das Handy ist entsperrt. Passwörter oder Schlüssel kann man vergessen – Finger, Auge & Co sind immer mit dabei. Biometrische Merkmale mögen auf den ersten Blick eine einfache Lösung sein, aber sicher sind sie nicht. Missbrauch wird Tür und Tor geöffnet (AK: Fingerprint, Augenscan & Co). Fingerlinien lassen sich nach einem Datendiebstahl nicht wie ein Schlüssel wechseln. Selbst Online-Fotos sind heikel, wie die Skandalfälle Clearview oder PimEyes zeigen: Millionen Profilbilder wurden nach biometrischen Merkmalen abgegriffen. Die EU-Kommission setzt leider bedenkliche Signale: der AIA erlaubt biometrische Fernidentifikation von Personen auf öffentlichen Plätzen unter bestimmten Voraussetzungen – ein gefährlicher Schritt in Richtung Massenüberwachung und weit entfernt von digitaler Fairness.

AK-Anliegen:

- Gerade im Konsument:innenbereich nehmen Biometrie-Anwendungen zu und damit – aufgrund des hohen Verkaufswerts der Daten – das Risiko der Zweckentfremdung, Identitätsdiebstahl und Datenmissbrauch. Biometrie darf daher kein Geschäft werden: Der Handel mit biometrischen Daten und die Weitergabe an externe Dritte sollte grundsätzlich verboten und mit hohen Strafen sanktioniert sein.
- Jede/r Konsument:in sollte selbst entscheiden können, ob seine/ihre biometrischen Daten verarbeitet werden dürfen oder nicht.
- Pflichtcheck vor dem Griff nach biometrischen Daten: Vor jedem Einsatz biometrischer Daten sollten Datenschutzbehörden angesichts des hohen Risiko- und Schadenspotenzials prüfen, ob die Verarbeitung biometrischer Daten notwendig und sinnvoll ist.
- Beim Onlinebanking oder Entsperren von Geräten dürfen biometrische Daten oder deren Hashwerte nicht gespeichert werden.
- Verbraucher:innen müssen Wahlrechte haben, wie sie sich authentifizieren wollen.
- Porträtbilder sind als sensible Daten einzustufen, um sie besser vor versteckter biometrischer Auswertung zu schützen.
- Gesichtserkennung ist jene Technologie, die aus heutiger Sicht die größte Bedrohung für Grundrechte und Demokratie darstellt. Technische Unzulänglichkeiten, etwa enorm hohe Fehlerraten, technologisch verschärfte Diskriminierung, Rassismus, Unterdrückung, Massenüberwachung und Verlust von Privatsphäre, Anonymität und persönlicher Freiheit sind Grund genug, enge rechtliche Grenzen zu ziehen.

Elektronische Identitätschecks nur wenn unbedingt nötig

Unternehmen ergreifen Sicherheitsmaßnahmen, um vor Betrug und Missbrauch geschützt zu sein. So wächst der Druck auf Verbraucher:innen, sich ständig elektronisch ausweisen zu müssen. Die für die Prüfung benötigten Daten sind aber ein bevorzugtes Angriffsziel für Identitätsdiebe. Datenschutz kommt zu kurz, wenn Konsument:innen auch bei Trivialgeschäften Identitätschecks durchlaufen müssen. Manche Prüfmethoden bringen Konsument:innen erst richtig in Gefahr: Wenn etwa Anbieter auf den Onlineversand von Ausweiskopien per Mail drängen – ein höchst unsicherer Weg für heikle Daten, die Kriminelle leicht ausspionieren können.

AK-Anliegen:

- Privacy-freundliche Vorschriften, wann und in welcher sicheren Form Identitätsprüfungen erlaubt sind. Der Gesetzgeber sollte nach deutschem Vorbild die Erstellung von Ausweiskopien nur unter bestimmten Voraussetzungen erlauben. Außerdem muss zum Schutz vor Missbrauch jede Ausweiskopie als solche (etwa mit Wasserzeichen) gekennzeichnet sein.
- Die EU strebt mit der Überarbeitung der EIDAS-Verordnung eine E-ID für alle EU-Bürger:innen an. Das als Konkurrenzmodell zu Apple, Google und Co gedachte EU-Vorhaben stößt auf massive Kritik: Eine Verbraucher:innen permanent zugewiesene Kennung ist strikt abzulehnen. Denn sie ermöglicht lebenslanges Profiling durch den Einsatz der E-ID bei allen nur denkbaren kommerziellen und behördlichen Kontakten. Digitale Fairness bedeutet: bereichsspezifische Abgrenzungen und neu zu generierende Kennungen bei jedem Einsatz der E-ID.

Kontaktieren Sie uns!

In Wien:

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

In Brüssel:

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

Bundesarbeitskammer Österreich
Prinz-Eugen-Straße 20-22
1040 Wien, Österreich
T +43 (0) 1 501 65-0

www.arbeiterkammer.at

AK EUROPA
Ständige Vertretung Österreichs bei der EU
Avenue de Cortenbergh 30
1040 Brüssel, Belgien
T +32 (0) 2 230 62 54

www.akeuropa.eu

Über uns

Die Bundesarbeitskammer (AK) ist die gesetzliche Interessenvertretung von rund 3,8 Millionen Arbeitnehmer:innen und Konsument:innen in Österreich. Sie vertritt ihre Mitglieder in allen sozial-, bildungs-, wirtschafts- und verbraucherpolitischen Angelegenheiten auf nationaler sowie auch auf der Brüsseler EU-Ebene. Darüber hinaus ist die Bundesarbeitskammer Teil der österreichischen Sozialpartnerschaft. Die AK ist im EU-Transparenzregister unter der Nummer 23869471911-54 registriert.

Die Aufgaben des 1991 eröffneten AK EUROPA Büros in Brüssel sind einerseits die Repräsentation der AK gegenüber europäischen Institutionen und Interessensorganisationen, das Monitoring von EU-Aktivitäten und die Wissensweitergabe von Brüssel nach Österreich, sowie gemeinsam mit den Länderkammern erarbeitete Expertise und Standpunkte der Arbeiterkammer in Brüssel zu lobbyieren.