BAK-POSITIONSPAPIER ZUR KONSULTATION DER EU-KOMMISSION ZUR DIGITALEN FAIRNESS

Februar 2023

AK WIEN
GERECHTIGKEIT MUSS SEIN

Digitale Fairness

Zum Hintergrund

Die EU-Kommission prüft mit ihrer Initiative (Konsultation bis 20.2.2023), ob EU-Verbraucherrecht **„Digitale Fairness“** gewährleistet. Aus Sicht der Bundesarbeitskammer (BAK) 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 BAK vermisst immer öfter einen fairen Umgang - im Sinne von Offenheit, Respekt und Selbstbestimmung - gegenüber Internetnutzerinnen. Wie noch zu zeigen ist, ist diese Entwicklung nicht nur für Konsument:innen, sondern auch für freie, demokratische Gesellschaften fatal.

Digitale Fairness ist ohne **„digitale Souveränität“** undenkbar. Konsument:innen wollen keinen undurchsichtigen Onlinetaktiken ausgeliefert sein, die ihre Autonomie untergraben. Fairness und Souveränität ergeben sich nicht von allein. Dafür sind die Kräfte- und Wissensungleichgewichte zwischen den Beteiligten zu groß. Die BAK freut sich über sich abzeichnende Rechtsanpassungen im bestehenden Rechtsrahmen (Verbraucherrechte RL, Unlautere Geschäftspraktiken-RL und missbräuchliche Klauseln-RL). Sie macht aber kein Hehl daraus, dass massive Interventionen des EU-Gesetzgebers nötig sind, um Verbraucherschutzdefizite im vorgelegten bzw schon beschlossenen EU-Digitalpaket auszugleichen und digitale Fairness als Standard durchzusetzen.

Denn **Verbraucherschutz 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.

Vor diesem Hintergrund erwartet die BAK von einer Initiative für digitale Fairness Anstrengungen, die **„digitale Menschenwürde“** von Konsument:innen (und Bürger:innen) zu sichern. 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. Wenn der Staat bspw Gesundheitsdaten von Konsument:innen, die von smarten Fitnessarmbändern erzeugt werden, pseudonymisiert für eigene Zwecke (Politiksteuerung, Gesundheitswesen, Wissenschaft) auswerten möchte. Oder wenn an Mobilitätsdaten, die von smarten Autos erzeugt werden, staatliche Stellen, die Verkehrsströme lenken, ebenso interessiert sind wie private Versicherungen, die Unfallhergänge prüfen wollen. Damit entstehen völlig neue Abhängigkeiten und Überblick, Verständnis der Tragweite und Selbstbestimmung von Konsument:innen gehen verloren. Die Folgen der Ausbeutung von Daten aus den Internetzugängen, Smartphones, sozialen Medien, Smart Homes, Fahrzeugen, Bezahlsystemen, elektronischen Bürgerservices und Gesundheitsdiensten gehen weit über das hinaus, womit Konsument:innen im Umgang mit Unternehmen und Behörden rechnen. Unternehmen bekommen Daten aus staatlichen Quellen (siehe Data Governance Act) und umgekehrt (siehe Data Act). Die Frage nach der digitalen Souveränität der Verbraucher:innen / Bürger:innen wurde dabei komplett ausgespart.

…das EU-Digitalpaket vergisst auf die Interessen der Konsument:innen: Wenn etwa das Künstliche Intelligenz Gesetz (AIA) KI-Hersteller Infopflichten gegenüber kommerziellen KI-Nutzer:innen auferlegt, aber keinerlei Transparenzpflichten gegenüber von KI betroffenen Konsument:innen enthält (Ausnahme: Kennzeichnungspflicht von Chatbots und Emotionserkennung). Oder wenn etwa der Data Act Konsument:innen ein Zugangsrecht zu den Betriebsdaten ihrer smarten Haushaltsgeräte (in Echtzeit) einräumt, aber kein Entscheidungsrecht, wer die Daten wie, wofür nutzen darf und wer 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. Marktkontrollen bieten ebenso wenig Schutz: Behörden wissen oft nicht mehr als die Konsument:innen und die Aufsichtsaufgaben stehen außer Verhältnis zu ihrer Ausstattung und ihrem Fachwissen. Mit dem geballten Wissen über Lebensgewohnheiten, Eigenschaften und die psychische Verfassung einer Person, kombiniert mit neurologischen Erkenntnissen, KI-basierten Prognosen und der technischen Gestaltung des Interface-Designs (Schnittstelle zum Kontakt mit Verbraucher:innen) können Unternehmen, deren Aufmerksamkeit und Entscheidungen lenken und manipulieren. Denn die Wissensasymmetrien waren noch nie größer: Das technologische Anwenderwissen von Vebraucher:innen ist idR gering, der Wissensvorsprung der Anbieter in Bezug auf die eingesetzte Technik dagegen immens. Kommerzielle Kommunikation über Websites, Apps, sonstige Schnittstellen bedeutet für Konsument:innen sehr oft informationelle Überforderung und in der Folge auch Übervorteilung.

…die Selbstbestimmung der Menschen steht auf dem Spiel: Beeinflussungs- und Suggestionspotential weisen zwar auch klassische Werbe- und Vertriebstechniken 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. Die von ihr beauftragte Studie “Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation” beschäftigt sich mit einem Teilaspekt der ungebührlichen Beeinflussung von Internetnutzer:innen durch „dark patterns“. Der Studie zufolge reicht der aktuelle Rechtsrahmen (und sein Vollzug) nicht aus, um Konsument:innen vor einer ihnen nicht bewussten Beeinflussung ihrer Entscheidungen zu schützen.

Konsument:innen werden über ihre (kognitiven, psychologischen) „Schwachstellen“ zunehmend effektiver zu Transaktionsentscheidungen bewegt, die ihren Interessen zuwiderlaufen. Entscheidend ist aus BAK-Sicht, dass nicht nur unseriöse Praktiken selbst verboten werden. Unternehmen sollten auch keine Vorbereitungshandlungen setzen dürfen, etwa Konsument:innen zu tracken und ihr Verhalten individuell (bzw in Form von Clustern oder statistischen Zuordnungen) zu analysieren.

Der Fitness-Check des Verbraucherrechts bietet die einmalige Chance, machtlose Konsument:innen (Bürger:innen) einer von digitalen Technologien beherrschten Welt zu selbstbestimmten Akteuren zu machen. Das auf Innovation ausgerichtete EU-Digitalpaket – bestehend ua 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 Act – muss durch korrespondierende digitale Verbraucherrechte besser ausbalanciert werden. So fehlen etwa durchsetzbare Rechtsansprüche auf eine Offline-Nutzung (wenn Kernfunktionen eines Produktes keine Internetverbindung benötigen). Oder auf eine allgemeine Beachtung von „Don’t Track“-Willenserklärungen (wenn Betroffene generell kein Verhaltenstracking wünschen und der Nutzung anwendungsbezogener, unwirksamer Cookie-Management-Systemen müde sind). Oder auf Werkzeuge, über die Datenflüsse beim Internet der Dinge für Konsument:innen leicht steuerbar sind uvm.

Die einzelnen BAK-Anliegen: Digitale Fairness bedeutet….

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

Was bedeutet Fairness in Bezug auf den AIA, Data Governance Act, Data Act usw? Die BAK 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 Verbrauchergesetzgebung. Verbraucher:innen wären die Verlierer:innen eines solchen Konzeptes. Ein halbes Dutzend Rechtsakten beinhalten de facto bereits den Vorrang für die Datenverwertung gegenüber den Geheimhaltungsinteressen der Verbraucher:innen.

BAK-Forderung:

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

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

Das Positionspapier des EU-Verbraucherverbands BEUC wird umgesetzt

„Towards European Digital Fairness“ (2/2023) enthält unzählige exzellente Forderungen und Verbesserungsvorschläge.

BAK-Forderung:

Die EU-Kommission sollte alle Vorschläge aufgreifen.

Marktkonzentration wird nicht erst spät ins Visier genommen

Denn dann ist sie schwer zu beseitigen. So weist die EU-Kommission bspw auf Amazons besorgniserregende Vormachtstellung bei Sprachassistenten hin. Dieser baut seine Dominanz bei Smart Homes gerade aus (https://germany.representation.ec.europa.eu/news/internet-der-dinge-fur-verbraucher-eu-kommission-veroffentlicht-abschlussbericht-uber-2022-01-20_de) und plant ua, eine Produktionsfirma für smarte Staubroboter (iRobot) zu übernehmen. Bei digitalen Autoassistenten entwickeln sich gerade ebenso ungehindert geschlossene Ökosysteme, die Verbraucherinteressen schaden. So können Autofahrerclubs, die Pannenhilfe leisten, auch bei simplen Batterieproblemen keine rasche Hilfe mehr vor Ort leisten. Fahrzeuge werden aufwändig und kostspielig in Werkstätten abgeschleppt. Denn Voraussetzung ist eine Internetverbindung, eigene elektronische Zugangsschlüssel für jeden Autotyp und manchmal auch die exklusiven Services einer Vertragswerkstätte. Der DMA (mit seinen verbrauchrelevanten Art 5 und 6) reguliert nur große Gatekeeper und greift damit zu kurz. Es reifen auch kleine innovative Unternehmen in der schwer greifbaren Einflusssphäre der Internetkonzerne zu dominanten Nischenplayern heran.

BAK-Forderung:

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

Zugunsten von KMUs gibt es zu viele Ausnahmen bei Vorschriften, die auch dem Konsumentenschutz dienen. Dies ist nicht sachgerecht (siehe zB die Ausnahme von KMU beim Kreditscoring in Annex 3 des AIA). Konsument:innen leiden unter Rechtswidrigkeiten unabhängig von der Größe des Unternehmens. Auch Start-Ups können im Windschatten großer Konzerne (durch Förderungen, technische, universitäre Kooperationen) wichtige Marktnischen besetzen und sollten die Art 5 und 6 des DMA beachten müssen.

Abkehr vom Leitbild des informierten Verbrauchers

Die Annahme, dass Verbraucher 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. Desinformation durch ausufernde Produkt- bzw Datenschutzinfos und Nutzungsbedingungen steuert auf neue Rekorde zu. Konsument:innen reagieren darauf mit Nichtbeachten und bestätigenden Klick, alles zur Kenntnis genommen zu haben. 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, 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.

BAK-Forderung:

Manipulationen (subjektive Absicht wie objektive Wirkung) muss per se verpönt und unzulässig sein, ganz unabhängig von der individuellen Lage des Verbrauchers. Der permanent verletzbare Verbraucher muss in der Gesetzgebung und Rechtsprechung an die Stelle des Leitbilds des durchschnittlich (informierten, verständigen, sorgfältigen usw) Verbrauchers 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 liegen in Vollzugsdefiziten, vor allem aber in Unzulänglichkeiten der DSGVO selbst. Nach einer Eurobarometerumfrage wünschen sich 92 % der Befragten Vorrang des Datenschutzes vor wirtschaftlichen Interessen. 78 % meinen, Onlineanbieter besitzen viel zu viele Kundendaten und 73 % wollen immer um Zustimmung zur Datennutzung gefragt werden. Erfüllte die DSGVO diese Hoffnung? Entscheiden Konsument:innen aktuell selbstbestimmter über ihre Daten? Wurde dem Anliegen, immer nach einer Zustimmung gefragt zu werden, entsprochen? Die Marktentwicklung der letzten Jahre geht in Richtung einer Datenökonomie, die das Selbstbestimmungsrecht von Verbraucher:innen unakzeptabel aushöhlt.

Überlange, nichtssagende Datennutzungsinfos, unübersichtliche Datenschutzvoreinstellungen, unpräzise, unüberprüfbare Auskünften, Datenverarbeitungen ohne Zustimmungen, weil sie im – schwer überprüfbaren – überwiegenden berechtigten Interesse des Unternehmens oder Dritter erfolgen, undurchsichtige algorithmische Entscheidungen, die angeblich nicht „ausschließlich“ sondern „nur“ teilweise automatisiert sind oder die nicht mit rechtlichen oder „erheblich“ beeinträchtigenden Folgen für die Verbraucher:innen verbunden sind, unlimitierte oder lange Speicherdauern, wobei was an Zeitdauer “erforderlich“ ist, Datenschutzbehörden völlig uneinheitlich beurteilen. Dem Wunsch nach physischer Datenlöschung wird nicht entsprochen: Verbraucher:innen müssen sich mangels Rechtsanspruchs oft mit einer Anonymisierung zufriedengeben. Ob und wie verlässlich anonymisiert wird, löst bei den Konsument:innen berechtigtes Misstrauen aus. Mangels einzuhaltender Standards und Nachweise können sie sich nie darauf verlassen, dass Daten nicht doch auf ihre Person rückführbar sind.

Zustimmungserklärungen sind selten, denn Unternehmen haben andere Trumpfkarten: sie stützen sich auf diffuse Erlaubnistatbestände wie „überwiegende berechtigte Verarbeitungsinteressen“, „vertraglich vereinbarte oder gesetzlich vorgesehene algorithmische Entscheidungsfindung“, Privilegien für „Statistik, Wissenschaft und Forschung“ und eine bequeme Rechtgrundlage im KI-Gesetz fürs Trainieren von KI in verharmlosend bezeichneten „Sandkästen“. Diese Rechtsgrundlagen höhlen digitale Selbstbestimmung weitgehend aus.

Algorithmisch wird über Bonität, die Wahrscheinlichkeit eines Zahlungsausfalls oder Missbrauchs von Konsument:innen entschieden. Digitale Fairness bedeutet, dass dieser massive Grundrechtseingriff im Detail fair reguliert wird. Scoring sollte auf Geschäftsfälle mit relevanten Ausfallsrisiken (Kredite, Ratenzahlung) beschränkt werden und bei geringfügigen Alltagsgeschäften unzulässig sein. 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.

BAK-Forderungen:

Durchdachte Lösungen liegen längst am Tisch.

Hierzu verweisen wir auf den Erfahrungsbericht und die Anliegen der BAK: AK-Stn_zur_Evaluation_der_Datenschutz-Grundverordnung.pdf (arbeiterkammer.at) sowie auf das Gutachten im Auftrag des Bundesverbands der Verbraucherzentralen (Evaluation der DSGVO aus Verbrauchersicht, Projektgruppe verfassungsverträgliche Technikgestaltung, Univ.-Prof. Dr. A. Roßnagel, 26.11.2019; https://www.vzbv.de/sites/default/files/downloads/2019/12/04/19-11-26_gutachten_evaluation_dsgvo.pdf).

Fairness by Design als Maxime

Die DSGVO enthält ein Recht auf „Privacy by Design". Was dieses Recht auf vorteilhafte Datenschutz-Voreinstellungen und Auswahlmöglichkeiten beinhaltet, ist – abgesehen von ein paar mitgliedsstaatliche Gerichtsentscheidungen – unklar. Cookie-Management-Systeme hat dieser Rechtsanspruch jedenfalls nicht verbraucherfreundlich determiniert: sie gelten als Paradebeispiel für Dark Patterns (siehe die Beschwerden des Datenschützers Max Schrems bezüglich mehr als 700 Websites: Cookie-Banner | noyb.eu). Ein ähnlicher Rechtsanspruch auf faire, neutrale Gestaltung aller digitalen Schnittstellen zwischen Unternehmen und Verbraucher:innen ist denkbar für Benutzeroberflächen, Architektur und Navigation bei Apps, Webseiten, IOT-Geräten usw. Es braucht aber mehr Ambition als in der DSGVO, diese Maxime durch klare Ge- und Verbote praxistauglich zu regeln.

BAK-Forderung:

Der Grundsatz „Fairness by Design" ist einzuführen, aber unbedingt durch gängige Gestaltungspflichten zu präzisieren. Er beinhaltet die Pflicht zu einem neutralen Design bzw Website-Architektur, um zu garantieren, dass Konsument:innen nicht mit kalkulierten psychologischen Tricks in die Irre geführt werden. Nicht nur Onlineanbieter an der direkten Schnittstelle zu Verbraucher:innen sind Adressaten, sondern auch dahinterstehende Dienstleister in der Wertschöpfungskette, die derzeit Dark Patterns als Services verkaufen und so zu ihrer massiven Verbreitung beitragen. Auch diese dürfen keine Software in Verkehr bringen, die den Designvorgaben widersprechen.

Dark Patterns umfassend verbieten

‚Dark Patterns' sind zwar zum Teil nach der Unlauteren Geschäftspraktiken RL bereits verboten. 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 („Nur noch 2 verfügbar!": EU-Kommission kritisiert manipulative Tricks von Onlineshops (netzpolitik.org),) setzten 40 Prozent der untersuchten Onlineshops auf Design-Tricks.

Die häufigsten Manipulationen: versteckte Informationen, falsche Hierarchien, nachteilige Vorauswahlen, Bedrängen (zB durch Countdown-Timer oder zeitlich begrenzte Angebote), erschwerte Stornierungen und erzwungene Registrierung. Unseriöse Techniken kommen bei mobilen Apps und Websites mit EU- oder Nicht-EU-Provenienz gleichermaßen vor. Laut der von der EU-Kommission beauftragten Studie ist das Bewusstsein der Verbraucher:innen für diesen Verlust an Souveränität genauso wenig ausgeprägt, wie die Fähigkeit, diese Praktiken im Alltag zu erkennen. Noch bedenklicher: Verbraucher:innen scheinen unlautere Praktiken als normale Interneterfahrung zu akzeptieren und sich an sie zu gewöhnen.

Was genau von diesem Begriff umfasst ist, ist leider mehr als unklar. Denn Werbe- und Vertriebsformen bezweckten schon immer, bei Verbraucher:innen Begehrlichkeiten zu wecken und zu Spontankäufen zu verleiten. Wo liegen die Grenzen zur verpönten Manipulation?

Das Digitale Dienste Gesetz erwähnt etwa schwer änderbare Standardeinstellungen oder Täuschungen, um Nutzer:innen zu Transaktionen zu drängen. Anbieter dürfen ihren Online-Marktplatz nicht so gestalten, dass Konsument:innen in ihrer „Autonomie, Entscheidungsfreiheit oder Wahlmöglichkeit beeinträchtigt“ werden. EG 67 beschreibt nicht abschließend einige der als Dark Patterns identifizierten Praktiken:

- Auswahlmöglichkeiten stärker hervorheben, wenn Nutzer zur Auswahl aufgefordert werden oder wiederholte Aufforderung, eine Auswahl zu treffen, wenn diese bereits getroffen wurde.
- Die Stornierung eines Dienstes erheblich umständlicher zu gestalten als die Anmeldung.
- Wahlmöglichkeiten schwieriger oder zeitaufwendiger gestalten als andere.
- Es unverhältnismäßig schwierig machen, Käufe abzubrechen oder sich von einer bestimmten Online-Plattform abzumelden.
- Nutzer in die Irre führen, indem sie zu Entscheidungen bezüglich Transaktionen verleitet werden oder die Entscheidung der Nutzer durch Standardeinstellungen, die sehr schwer zu ändern sind, unverhältnismäßig zu beeinflussen.
- Zeitlicher Druck (Countdowns, Zahl anderer Interessent:innen, geringe Zahl verfügbarer Stücke) und inhaltlicher Druck (Drohung mit Beeinträchtigung des „Nutzererlebnisses“)

BAK-Forderungen:

- Die im zitierten EG 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 genauen Grenzen zu zulässigen Formen der Suggestivwerbung aufzuzeigen, um 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 finanziellem Schaden, 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 (in eventu eine Aufnahme in die UWG-RL als unlautere Geschäftspraktik).
- EU-weite gemeinsame Initiativen zum wirksamen Vollzug der RL über unlautere Geschäftspraktiken samt EU-Datenbank nationaler Dark-Patterns-Entscheidungen und Best-Practice-Leitlinien der EU-Kommission.
- 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 (CRD) zur verpflichtenden Bereitstellung einer Schaltfläche zur Vertragsauflösung, die eine Vertragskündigung genauso einfach machen soll, wie die Zustimmung zum Vertragsabschluss.

Immateriellen Schaden pauschal ersetzen

Verbraucher:innen brauchen über ihre wirtschaftlichen Interessen hinaus Schutz. Der Verlust an Autonomie durch Desinformation, geringe Entscheidungsfreiheit und das Gefühl der Entmachtung ist ebenso relevant. Zur Abgeltung von Personen,- Sach- und Vermögensschäden sollten daher auch immaterielle Schäden hinzukommen. Der Unrechtsgehalt von Verstößen gegen die digitale Fairness (zB Diskriminierung durch personalisierte Preise), Selbstbestimmung (zB Übermittlung pseudonymisierter Gerätedaten ohne Einwilligung) und Menschenwürde (zB Einsatz von Emotionserkennung) sollte dadurch betont werden, dass den Betroffenen dafür pauschalierte Schadenersatzbeträge gebühren.

BAK-Forderung:

Da mangelnde digitale Fairness oft keinen einfach bewertbaren Schaden hinterlässt, sollten Betroffene immaterielle Schäden pauschal (Mindestsätze) abgegolten bekommen. Das KI-Gesetz berücksichtigt wiederum nur Personenschäden und Grundrechtsverletzungen: Vermögensschäden und Fairnessverletzungen, die keine Grundrechtsverstöße im engeren Sinn sind, müssen ebenfalls abgegolten werden.

Menschenwürde bewahren

Einige der sich derzeit ungebremst entwickelnden Trends sind mit den europäischen Grundrechten gar nicht in Einklang zu bringen, sondern 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 (Gesichtserkennung im Einsatz gegen unliebsame Anwaltskanzleien - Überwachung - derStandard.at › Web). PimEyes und Clearview AI sind Unternehmen, die ungefragt Millionen von Gesichtsbildern aus dem Internet speichern, biometrisch auswerten und katalogisieren, um daraus Überwachungssysteme zu bauen (PimEyes – Verlust der Anonymität (datenschutz-notizen.de). KI errechnet für Anbieter von Onlinespielen anhand der Mimik bzw des Tastendrucks der Spieler deren momentane Gefühlszustände, um auf dieser Basis Spielfiguren zu personalisieren, aber auch im richtigen Moment zu Werbung oder dem nächsten Spiellevel zu schalten (GaCha 2019: Die Top 3 Emotion AI Spielkonzepte - audEERING Emotionale KI: Berechnete Gefühle (netzpolitik.org)) Zoom: Bürgerrechtler warnen vor Emotions-Scanner bei Videokonferenztool - DER SPIEGEL)

BAK-Forderung:

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

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

Digitale Sorgfaltspflichten für Gewerbetreibende

Auch im Gewerberecht muss „digitale Fairness“ einziehen. Die Ausübungsregeln und Sorgfaltspflichten vieler Branchen entsprechen nicht der Digitalisierung und damit auch nicht dem aktuellen Konsumentenschutzbedarf. Völlig ignoriert wurde bislang, dass neben dem Diensteanbieter, der im direktem Kontakt mit Verbraucher:innen steht, noch eine Fülle anderer Dienstleister bzw Vermittler in der Wertschöpfungskette (Distribution von Onlinewerbung, Softwareerstellung für standardisierte Webshops, Cookie Management Systeme uvm) beteiligt sind. Diese werden für rechtswidriges Handeln so gut wie nie zur Verantwortung gezogen. Dabei führen ihnen zurechenbare Rechtsverstöße zu verbreiteten Streuschäden, wenn zigtausende Onlineanbieter deren Dienste nutzen. Behörden, Gerichte und Verbraucherschützer müssten sich nicht mit millionenfach kopierten unlauterem Onlinevertriebs- und Werbeverhalten befassen: denn das Problem ließe sich auf der Ebene der wenigen dahinterstehenden Firmen oft leichter beheben.

BAK-Forderung:

Auch im Gewerberecht sollte die Bedachtnahme auf ein neutrales Webseitendesign, Verantwortung für eingebettete Drittwerbung und Drittanbietercookies, hohe Verschlüsselungsstandards und andere Cybersicherheitsmaßnahmen im Kundenverkehr verankert und einer Aufsicht unterworfen werden.

Personalisierte Preise verbieten

Verhaltensprofile und KI machen auf den einzelnen Verbraucher in Echtzeit zugeschnittene Preise möglich. Dank der Modernisierungs-RL haben Unternehmen zwar darauf hinzuweisen, dass sie personalisierte Preise nutzen. Betroffene wissen dann 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 personenbezogenen Daten (nicht statistischen Zuordnungen), rechtliche Folgen und dass die Auskünfte keine Geschäftsgeheimnisse berühren. Für Verbraucher:innen bedeutet dies den Verlust des Gefühls für den „Normalpreis“ oder Referenzpreises und den Eindruck von Willkür (bei bloßem Verweis auf den Algorithmus) und ein Gefühl der Ohnmacht (https://zivilrecht.univie.ac.at/fileadmin/user_upload/i_zivilrecht/Wendehorst/03_Peter_Rott_Wien_Personalisierte_Preise_.pdf). Personalisierte Preise bestehen kaum einen Fairness-Check, brechen mit berechtigten Verbrauchererwartungen auf grundsätzlich gleiche Zahlungsbedingungen für gleiche Leistungen und stellen das Kartellrecht punkto Nachweis von Marktmachtmissbräuchen vor große Herausforderungen (siehe die Bedenken der Wirtschaftsuniversität Wien 06_Robertson_Personalisierte_Preise_im_Kartellrecht_2022.pdf (univie.ac.at)).

BAK-Forderung:

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

Künstliche Intelligenz ist wirklich vertrauenswürdig

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 (siehe ITA-Studie für Arbeiterkammer: Entmündigung durch Künstliche Intelligenz? (oeaw.ac.at) und Kuenstliche_Intelligenz_aus_Verbrauchersicht.pdf (arbeiterkammer.at)). Inforechte 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 wohl auch nicht anderswo reguliert werden. Hohes Risiko bedeutet nicht hohes Schutzniveau: Statt Kontrollen durch unabhängige Behörden dürfen sich die meisten Hersteller einfach selbst prüfen.

Der Verbraucheralltag wird aber viel mehr von KI beeinflusst, als der AIA zugesteht. Dieser zählt nur Bonitätscorings, Risiko- und Prämienkalkulationen bei Lebens- und Krankenversicherungen und biometrische Fernüberwachung – überdies mit Einschränkungen - zu den hochriskanten Anwendungen. Konsument:innen werden aber auch algorithmisch bewertet bei KFZ-Versicherungen, bei Verhaltensmustern, die zB Haushaltsversicherungen als Missbrauch deuten, bei personalisierten Angeboten und Preisen, bei Inhaltsempfehlungen uvm. KI kann in smarten Geräten dazu dienen, das Alltagsverhalten massenhaft zu überwachen, aus bereits anonymisierten Datensätzen Einzelpersonen wiedererkennen, als Informationsfilter Meinungsvielfalt bedrohen und Konsument:innen, diskriminierenden Prognosen aussetzen bzw Gruppen zuordnen.

Sogenannte „Sandkästen“ oder „Reallabore“ machen Konsument:innen zu Versuchskaninchen: Unternehmen können KI beaufsichtigt von einer Behörde vor der Marktreife testen, ohne Rechtsvorschriften beachten zu müssen. Sind dafür personenbezogene Trainingsdaten nötig, muss der Sandkasten im öffentlichen Interesse sein und ua der Gesundheit, Umwelt, der öffentlichen Verwaltung dienen. Digitale Fairness gibt es keine: betroffene KonsumentInnen können über ihre Teilnahme nicht frei entscheiden: sie werden weder informiert noch nach ihrer Zustimmung gefragt.

BAK-Forderungen:

- Egal ob nur Algorithmus oder schon KI: der AIA 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 Konsument:innen / Bürger:innen auf Information, Nachvollziehbarkeit, Auskunft, Autonomie, KI-Entscheidungen auch abzulehnen sowie Beschwerderechte. Denn 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 bzw Nutzer 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 einwilligen (bei hohem öffentlichem Interesse kann die Genehmigung von Datenschutzbehörden Einzeleinwilligungen ersetzen).
- Ge- und Verbote zum Schutz von Minderjährigen sind einzuführen. Wir verweisen auf die Vorschläge im Rechtsgutachten der Universität Wien (Christiane Wendehorst) abrufbar unter Informationen zur Konsumentenpolitik in Österreich (sozialministerium.at)
- Verbandsklagsbefugnis für Verbraucherverbände

Kein Social Sorting durch Scorings

Der 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 sollen und 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. Wie unterschiedlich deren Arbeitsweise (trotz der Harmonisierung durch die DSGVO) ist, ist erschreckend. Wirtschaftsauskunfteien speichern Konsument:innendaten in Österreich bis zu 10 Jahren, in Deutschland gelten sie nach 3 Jahren als nicht mehr aussagekräftig und werden gelöscht.

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.

BAK-Anliegen:

- Digitale Fairness bedeutet, dass Wirtschaftsauskunfteien und Scoringverantwortlichen konkrete Qualitätsnormen auferlegt werden.
- Social Scoring ist ausnahmslos zu verbieten. Es darf an das deutsche "Volkszählungsurteil" von 1983 erinnert werden: *"Eine Rechtsordnung, in der niemand mehr wissen kann, wer was, wann und bei welcher Gelegenheit über einen weiß, wäre mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar. Wer unsicher ist, ob abweichendes Verhalten irgendwann einmal notiert und dauerhaft als Information gespeichert, genutzt oder weitergegeben wird, wird versuchen, nicht durch ein solches Verhalten aufzufallen. Dies würde nicht nur die Entwicklungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, denn Selbstbestimmung ist eine elementare Funktionsbedingung eines freiheitlich-demokratischen Gemeinwesens, das auf der Handlungs- und Mitwirkungsfähigkeit seiner Bürgerinnen und Bürger beruht."*

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 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 aber nur dann, 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.

BAK-Anliegen:

- Der DSA regelt, wann Plattformen nicht haften. Es braucht auch Haftungsgrundsätze, wann Onlinemarktplätze für Rechtswidrigkeiten von Drittanbietern haften.
- Konsument:innen dürfen darauf vertrauen, 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 (https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Online_Platforms.pdf). Danach greift die gesamtschuldnerische Mithaftung des Plattformanbieters, wenn die Plattform Sorgfaltspflichten missachtet oder der Konsument „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.

Transparentes „Dropshipping“

Dropshipping ist eine an sich legitime Logistik-Variante, bei der die Ware vom Hersteller oder einem Großhändler direkt an die Konsument:innen geschickt wird, ohne dass die Händler diese selbst lagern. Das Problem ist, dass zunehmend unseriöse Anbieter dieses Modell nutzen. Vielfach wird mit EU-Adressen suggeriert, dass Konsument:innen direkt bei einem europäischen Onlinehändler, der über eigene Warenlager verfügt, kaufen. Tatsächlich suchen Dropshipper nach Eingang einer Bestellung erst nach geeigneten Lieferanten im asiatischen Raum. Dies führt häufig zu extrem langen Lieferzeiten, Lieferausfällen und krassen Abweichungen der gelieferten von der bestellten Ware.

BAK-Forderung:

Die Infopflichten der Verbraucherrechte-RL sind zu ergänzen: Plattformen und Onlinehändler müssen gut sichtbar machen, wenn sie Dropshipper ohne eigenen Warenbestand sind.

Richtige Kundenbewertungen 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.

BAK-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 Dienste 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. Zuboff warnte schon 2018 vor einer Überwachung zur Kapitalisierung von Nutzerdaten bei gleichzeitiger Entmündigung ihrer eigentlichen Besitzer. Und war damit durchaus prophetisch. Immer mehr im Alltagsleben verwendete Objekte sind miteinander vernetzt. So können etwa Alarmanlagen, Backrohre und Mähroboter über das Internet gesteuert werden, oft auch ohne direktes Zutun eines Menschen. Auch Smart-Fernseher und Smart-Cars sind längst Realität. Gegenstände, die ins Internet integriert sind, erlauben Firmen noch tiefere Einblicke in unser Leben – das Erstellen von Persönlichkeitsprofilen oder Prognosen über künftiges Verhalten inbegriffen. 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. Es zeichnet sich ein krasses vertragliches Ungleichgewicht in den Rechtspositionen zwischen IoT-Anbietern und ihren Kunden ab. 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.

So gab die smarte „Spionage“-Kinderpuppe Cayla über ihre Spracherkennungsfunktion nicht nur nette algorithmen-gesteuerte Antworten auf Fragen von Kindern sondern belauschte auch deren sonstigen Gespräche. Der US-Traktorenhersteller John Deere versuchte seinen Kunden das Eigentum und die Reparaturrechte an ihren softwarebasierten Maschinen abzusprechen. Erst heuer wurden die Begehren des IoT-Anbieters nach einem jahrelangen Prozess abgewiesen. Konsument:innen entrichten zwar einen „Kaufpreis“ und vermeinen damit Eigentümer am Produkt mit all seinen Komponenten geworden zu sein. Oft trifft das aber nur mehr auf das äußere Erscheinungsbild, also etwa das Gehäuse eines vernetzten Fernsehers oder die Karosserie eines Fahrzeuges, zu.

Das Innenleben ist software-dominiert und steht unter Eigentumsvorbehalt der Anbieter. Der bestimmungsmäßige Gebrauch wird durch Lizenzen geregelt. Was Nutzer damit anfangen können oder nicht, regeln die Anbieter einseitig zu ihren Gunsten (zB Gewährleistungsausschluss nach Reparaturen außerhalb von Vertragswerkstätten) und über technische Schranken (Digital Right Management Systeme). Daraus ergeben sich neue Abhängigkeiten.

Aktuell bieten Autohersteller (noch) getrennte Verträge an – einen für den Autokauf und einen weiteren, mit dem der Zugang zu Zusatzservices (Entertainment, Navigation uvm) gebucht wird. Noch kann jeder Besitzer frei entscheiden, ob er die Zusatzleistungen in Anspruch nehmen will, denn die Fahrfunktion ist davon unabhängig. Es besteht das Risiko, dass über kurz oder lang viele Funktionen nur mehr als Gesamtpaket erworben werden können. Denn Autohersteller sehen ihre Umsatzerwartungen in der Autoproduktion schwinden und verlegen ihre Anstrengungen auf Kundenbindung durch Services, die auf Abonnementzahlungen beruhen. Das wirtschaftlich erfolgreiche, geschlossene Ökosystem von Apple dient dabei als Vorbild. Im ungünstigsten Fall werden Kunden künftig vom Abschleppservice über Versicherungen und den Assistenten für (teil) autonomes Fahren bis hin zur Wartung fix an einen Hersteller gebunden sein (AK-Studie: https://www.arbeiterkammer.at/service/studien/konsument/Vernetzte_Automobile.html).

Zusammengefasste BAK-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 Verbraucher sich seine Werkstätte frei aussucht oder nicht alle anfallenden Daten zugänglich macht.
- Smarte Produkte müssen (de-)aktivierbare IoT-Funktionen haben und auch offline nutzbar sein.

Im Einzelnen: 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. Dieser Druck zu einem „always-on“ dürfte auch bei vielen IoT-Produkten entstehen. (siehe AK Studie: https://www.arbeiterkammer.at/beratung/konsument/Datenschutz/Online-Spiele_Spione_im_Kinderzimmer.html).

BAK-Anliegen:

Ohne ein explizit verankertes „Offline“- Recht werden Verbraucher nur die Wahl des „take it – or leave it“ (Akzeptiere oder verlasse das Angebot) haben. Digitale Souveränität bedeutet, Kernfunktionen eines Produktes – soweit technisch möglich – bei Bedarf auch offline nutzen zu können.

Im Einzelnen: Eigentum statt Lizenzen

Neue Geschäftsmodelle drängen auf den Markt. Statt dem Kauf mit vollständigem Eigentumsübergang werden immer öfter bloße Nutzungsrechte eingeräumt. Der Bezug kann einmalig sein, ein Dauerschuldverhältnis mit Abonnement, mit Geld oder Daten bezahlt werden. Die Geschäftsmodelle nehmen Anleihen bei den Nutzungsrechten von urheberrechtlich geschützten Werken. Vernetzte Produkte weisen eine starke Servicekomponente auf. Nur hinsichtlich einiger weniger Rechte, etwa auf Gewährleistung für einige (objektive) Anforderungen an das vernetzte Gerät, setzt die Warenhandels-Richtlinie Grenzen.

BAK-Anliegen:

- Die Eigentümerrolle der Konsument:innen ist im EU-Recht unbedingt zu stärken. Eigentümer können andere vom Zugriff auf ihr Eigentum ausschließen. Urheberrechtsinhaber können hingegen Lizenzerwerbern durch internetspezifische Überwachungsmethoden ungleich leichter „auf die Finger schauen“ und freie Werknutzungen unterbinden.
- Konsument:innen sollen frei entscheiden, wie, wie lange und wie anonym sie etwas nutzen, wem sie etwas leihen oder weiterverkaufen wollen. Sie dürfen auch keinen Kontrollen und Verboten unterliegen, wenn sie die Sache verändern, selbst reparieren oder reparieren lassen.

Im Einzelnen: Dem Data Act Verbraucherrechte 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 und 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 und wie groß die Wohnung ist?

BAK-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 Verbraucherbedürfnissen 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 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 einer Pandemie) können Datenschutzbehörden Allgemeingenehmigungen erteilen.

E-Privacy stärken statt aushöhlen

Die e-Privacy RL entspricht nicht mehr dem aktuellen Schutzbedarf der Konsument:innen gegen Überwachung ihres Verhaltens im Internet. Mit der Nachfolger-VO droht Konsument:innen aber eine Absenkung des Datenschutzniveaus. Internet- bzw Medienkonzerne und die Onlinewerbewirtschaft setzen sich gegen bessere Schutzstandards, die das Ausspähen des Internetnutzerverhaltens mit Cookies und anderen Techniken erschweren, mit aller Macht zur Wehr. Auch der EU-Vorschlag für Rechtsvorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern im Internet, ist ein Angriff aufs Kommunikationsgeheimnis. Die Onlineplattformen müssten Material über sexuellen Kindesmissbrauch in ihren Diensten aufdecken, melden und entfernen. Erfolgreiche Strafverfolgung darf aber keinesfalls bedeuten, dass der gesamte Kommunikationsverkehr unbeteiligter Konsument:innen Anbietern zugänglich und gefiltert wird.

BAK-Anliegen:

Digitale Fairness bedeutet, die e-Privacy RL nicht aufzuweichen. Das heißt: absolute Vertraulichkeit der Kommunikationsinhalte, aber auch der Schutz von Standort- und Verkehrsdaten vor kommerzieller Ausbeutung, aber auch staatlicher und wissenschaftlicher Analyse ohne Kenntnis und Zustimmung der Betroffenen. Auch der Schutz von Hardware der Verbraucher:innen vor Cookiezugriffen, Canvas-Fingerprinting und anderen Tracking-Techniken darf nicht gelockert werden. Verbraucher:innen müssen auf einfachere Weise als bisher (über Cookie-Management-Systeme) Tracking generell widersprechen können, ohne dass Funktionen und Zugänge (entgegen dem Koppelungsverbot der DSGVO) daraufhin für sie gesperrt sind.

Verpflichtende Investitionen in IoT-Sicherheit

IT-Sicherheit ist kostspielig. Ohne rechtliche Vorgaben wird zu wenig in Ausfallssicherung und Präventionsmaßnahmen gegen Internetkriminalität investiert und viele Risken den Verbraucher:innen aufgebürdet. Bei den elektronischen Assistenzsystemen einiger Autotypen gibt es immer wieder kritische Schwachstellen, durch die Hacker Fahrzeuge komplett fernsteuern konnten („Hacker steuern Jeep Cherokee fern“ Heise.de).

Auch das Bordsystem von BMW (ConnectedDrive) fand den Weg in die Schlagzeilen, nachdem der deutsche Verkehrsclubs ADAC die Türverriegelung der Fahrzeuge unberechtigterweise von der Ferne aufschließen konnte.

BAK-Anliegen:

- Sicherheit muss im Produkt verankert sein und in Bezug auf die Vernetzung über Schnittstellensicherheit technisch abgesichert werden (Safety by Design).
- Sicherheit darf keine optionale Zusatzleistung sein, die Konsument:innen extra erwerben müssen.
- Gefahren, die sich aus für Konsument:innen weitgehend unsichtbaren Softwareprozessen bei Automatisierung und vernetzten Systemen ergeben, müssen vom Hersteller und seinen Softwarelieferanten beherrscht werden.
- Solange es keine verbindlichen Normen zur IT-Sicherheit gibt, dürfen unklare Haftungssituationen nicht zulasten geschädigter Konsument:innen gehen. So weist der EU-Verbraucherverband BEUC darauf hin, dass es vielen IoT-Geräten an elementaren Sicherheitsmerkmalen, wie einer zeitgemäßen End-zu-End-Verschlüsselung, Zwei-Faktor-Authentifizierung oder zumindest Passwortschutz mangelt.
- Es müssen nationale Aufsichtsbehörden bestimmt werden, die gefährliche Produkte vom Markt rasch entfernen können.

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. Angesichts der geringen schadensvorbeugenden Anforderungen an KI im AIA, kommt dem Haftungsregime hohes Gewicht zu: Wirkt es so abschreckend, dass KI-Hersteller und -Nutzer größtmögliche Vorsicht walten lassen? Haben Personen, die dennoch zu Schaden kommen, einen möglichst niedrigschwelligen Zugang zur Entschädigung in Anbetracht der großen Wissensasymmetrien zwischen den Beteiligten? Die unbefriedigende Bilanz aus BAK-Sicht lautet: 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.

BAK-Anliegen:

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

Schutz vor personalisierter und manipulativer Werbung

Tracking verfolgt uns so gut wie bei jeder Onlineaktivität, in dem auf unsere Hardware, va Browserinfos, zugegriffen wird. Auf Basis unserer Durchleuchtung und unserer Profile werden uns individuelle Angebote und Werbung geliefert. Dieses System ist die Basis für Manipulation und Ausbeutung unserer Schwächen, aber auch von Desinformation, Hass und Hetze in sozialen Medien. Konsument:innen werden mit subtilen Tricks länger am Bildschirm gehalten und sehen immer extremere Inhalte, die die Gesellschaft spalten, aber durch hohe Klickraten gewinnbringend sind. Die Alternative ist kontextbasierte Werbung, die mit keinen Einnahmeverlusten verbunden ist (Beispiel: öffentlich-rechtlicher Rundfunk NPO in den NL, der von cookie- auf kontextbasierte Werbung umgestellt hat).

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 „Dont-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.

BAK-Forderungen:

Verbraucher:innen müssen losgelöst vom Alter sich 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.

Werbung unterliegt verschiedenen rechtlichen Rahmenbedingungen (Audiovisuelle Medien RL, eCommerce RL, Unfair Practices RL). Neben dem Schutzbedürfnis von Minderjährigen (zB keine direkte Kaufaufforderung an Kinder) bestehen vor allem Kennzeichnungspflichten bei bezahlten Werbeinhalten. Influencer:innen vernachlässigen nicht nur oft rechtliche Vorgaben (Vollzugsdefizit), oft ist unklar, wie diese Vorgaben auf den sozialen Plattformen zu erfüllen sind (fehlende Rechtssicherheit). Wie ist zB „Unboxing“, das Auspacken von Einkäufen vor der Kamera zu bewerten, wenn kein Entgelt dafür von Unternehmen floss? Reicht es, wenn mittels Hashtags („#“) auf Werbekooperationen aufmerksam gemacht wird. Es ist davon auszugehen, dass ein Hashtag „Werbung“ nicht genügt, damit ein Kind im Alter von neun Jahren auf ersten Blick erkennt, dass es sich nicht um einen redaktionellen Inhalt handelt.

BAK-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 ungesunder Lebensmitteln.
- 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 BAK hat allein 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.

Digitale Geheimhaltungsrechte bei Gesundheitsdaten

Der VO-Entwurf über einen Europäischen Gesundheitsdatenraum (EHDS) bezweckt,

- „Akteuren aus Forschung und Innovation, politischen Entscheidungsträgern und Regulierungsbehörden“ EU-weiten Zugang zu elektronischen Gesundheitsdaten zu verschaffen. Öffentliche wie private „Dateninhaber“ werden verpflichtet, für Zwecke der Gesundheitsversorgung erhobene Daten an eine „Zugangsstelle“ für Gesundheitsdaten herauszugeben, die diese Datennutzern auch in pseudonymisierter (mittelbar personenbezogener) Form EU-weit anbietet.
- die Gestaltung eines „echten Binnenmarkts für datenbasierte digitale Gesundheitsprodukte und -dienste“ und
- leichteren Zugang von Konsument:innen (Patient:innen) zu ihren elektronisch gespeicherten Gesundheitsdaten.

Digitale Fairness war nicht die Maxime des Entwurfes, denn

- die Schutzstandards der Datenschutzgrundverordnung (DSGVO) werden unterschritten.
- das Selbstbestimmungsrecht der von den beabsichtigten Verarbeitungen Betroffenen tritt pauschal und undifferenziert hinter die Verwertungsinteressen der Datenökonomie zurück.
- Betroffene könnten auf die Weiternutzung ihrer Gesundheitsdaten keinen Einfluss nehmen: ihnen stünde kein Einwilligungsrecht bzw Widerrufsrecht zu, obwohl ihre (mittelbar) personenbezogenen Daten für alle nur erdenklichen politischen, wissenschaftlichen und kommerziellen Projekte, an denen öffentliche Interessen bestehen bzw behauptet werden, ausgewertet werden dürfen.
- Auch eine Blankoermächtigung für den Abgleich mit Daten aus allen anderen Lebensbereichen in völlig unspezifischen „Notsituationen“ ist enthalten. Die Gesundheitsdaten, die für die Sekundärnutzung verarbeitet werden können, sollten „flexibel genug sein, um den sich wandelnden Bedürfnissen der Datennutzer gerecht zu werden, vor allem auch gesundheitsrelevante Einflussfaktoren umfassen“ (siehe EG 39). Dazu zählen:

- Daten aus dem Gesundheitssystem, wie elektronische Patientenakten, Daten zu Krankenversicherungsleistungen, Krankheitsregister, Genomdaten usw,
- sowie Daten zu gesundheitsrelevanten Einflussfaktoren wie zB Konsum bestimmter Substanzen, Obdachlosigkeit, Krankenversicherung, Mindesteinkommen, beruflicher Status, Verhalten...
- Auch von Personen selbst erzeugte Daten, zB Daten von Medizinprodukten, Wellness-Apps oder anderen tragbaren Geräten und digitalen Gesundheitsanwendungen, können dazugehören.
- Datennutzer dürfen die Daten auch mit ganz anderen Daten anreichern und sollten die „verbesserten" Datensätze dem ursprünglichen Dateninhaber kostenlos bereitstellen.
- Registerdaten, wie Impfregister uvm.

- Betroffene wüssten nicht, wer, wo, welche Daten, wofür und wie lange verwendet. Geht es nach der EU-Kommission, so entfällt nämlich die Informationspflicht nach der DSGVO darüber, wer, mit welchen meiner Daten für welchen Zweck Datenanalysen durchführt. Lediglich auf Websites sind allgemeinste Infos über erteilte Datengenehmigungen zu veröffentlichen. Das Recht aufgrund der DSGVO, detaillierte Auskunft verlangen zu können, wird nur bei der „primären Datennutzung" (für die Erbringung von Gesundheitsdiensten) explizit beschrieben. Bei der „sekundären Datennutzung" (Weiterverarbeitung für ganz andere Zwecke) wird dieses Recht schon dadurch faktisch beschnitten, dass Betroffene nicht einmal erfahren, in welchen der Datengenehmigungen ihre Daten stecken.
- Der Schutz gegen Datenmissbrauch wird im Entwurf nicht nennenswert geregelt. Zu den vagen Anforderungen zählt lediglich, dass die Zugangsstellen zu den Daten auf dem „modernsten" technischen Stand sein mögen. Das ist ein grober Sorgfaltsmangel: zentral abrufbare Datenbestände dieser Größe und von hohem Handelswert samt EU-weiten Zugriffen ziehen fast zwangsläufig missbräuchliche, kriminelle Praktiken an.

Die BAK-Anliegen:

- Eine DSGVO-widrige VO widerspricht digitaler Fairness und sollte massiv überarbeitet werden. Es darf keinen pauschalen Vorrang der Datennutzung vor den Geheimhaltungsinteressen der Betroffenen geben.
- Da es auch um Daten von Verbraucher:innen geht (Fitnesstracker uÄ), ist die GD für Konsumenten und Justiz in das Vorhaben gleichberechtigt zu involvieren.
- Will man das Vertrauen der Bevölkerung in die Nutzung ihrer Gesundheitsdaten etwa für Forschungszwecke nicht verlieren, ist ein Konzept nötig, das die DSGVO und insbesondere die Selbstbestimmung der Betroffenen achtet (Information und Einwilligung).
- Der Datenumfang ist viel zu umfangreich und unbestimmt**:** Das Zusammenführen sämtlicher Daten aus dem Gesundheitsbereich mit allen nur erdenklichen soziodemografischen Verhaltensdaten würde ein einzigartiges individuelles Verhaltensprofil ermöglichen, das bisherige kommerzielle Verhaltensprofile der Digitalwirtschaft in den Schatten stellt.
- Wer "Dateninhaber" ist, der seine Daten für die Weiterverarbeitung anbieten muss, wird nicht präzisiert: Der Kreis der Adressaten muss rechtssicher abgesteckt sein.
- Ein Rückschluss auf bestimmbare Einzelpersonen ist möglich. Dies muss verlässlich unterbunden werden: Betroffene müssten damit rechnen, dass sensibelste Daten, ganze Verhaltens- und Gesundheitsprofile sowie Zusammenhänge und Analysen daraus ihrer Person konkret zuordenbar sind. Der Entwurf enthält nicht nur keine diesbezügliche Schutzgarantie. Einzelne Bestimmungen und EGs gehen dezidiert davon aus, dass die Zugangsstellen zu Gesundheitsdaten, den Datenzugang in einer Weise ermöglichen, dass Rückschlüsse auf einzelne Personen denkbar sind.

- Digitale Fairness statt Selbstbestimmungsrechte komplett missachten: Nach Art 33 Abs 5 soll in jenen Fällen, in denen nach nationalem Recht die Einwilligung der Betroffenen erforderlich ist, sich die Zugangsstelle für Gesundheitsdaten bei der Gewährung des Zugangs einfach „auf die in diesem Kapitel festgelegten Pflichten“ berufen. Angesichts des grundsätzlichen Verarbeitungsverbotes von Gesundheitsdaten müssen Eingriffsnormen in das Grundrecht besonders präzise formuliert sein. Diese Anforderung erfüllt der Entwurf nicht. Informationsrechte für Betroffene nach der DSGVO werden einfach beseitigt, womit Betroffene von der Sekundärnutzung ihrer Daten in der Regel nichts erfahren und sich gegen mutmaßliche Rechtsverstöße auch nicht wehren können.
- Eine Vorabgenehmigungspflicht für Datenschutzbehörden einführen statt ihre Aufsicht faktisch auszuschalten. Neue „Zugangsstellen für die Datennutzung“ sollen die VO vollziehen und Datenzugriffe genehmigen. Ihr Aufsichtsziel ist, möglichst ungehinderten Datenzugriff EU-weit zu garantieren. Die Absicherung von Grundrechten zählt nicht dazu.
- Datengetriebene Forschung, Politiksteuerung und kommerzielle Innovationen stiften Nutzen, müssen aber grundrechtskonform sein. Die Nutzung ist auf anonymisierte, synthetische Daten oder solche, für die Zustimmungen der Betroffenen vorliegen, zu beschränken.
- Verarbeitungserleichterungen nur bei sorgsam geprüften, wichtigen öffentlichen Gesundheitsinteresse: So sollte grundsätzlich die Zustimmung jedes Einzelnen erforderlich sein. Weist der Datennutzer ein erhebliches öffentliches Interesse an seinem Forschungsgegenstand und seine fachliche Eignung nach, so könnte die Datenschutzbehörde die einzelnen Zustimmungen der Betroffenen durch ihre Genehmigung des Projektes ersetzen.
- Nennenswerte Sicherheit und Sanktionen fehlen. Sie sind aber als „Digitale Fairness“-Maßnahmen undabdingbar: Ein derart zentralisierter Ansatz, der den Austausch von Daten aus unzähligen, voneinander getrennten sensiblen Anwendungen zum Ziel hat, entspricht aufgrund der leichten Angreifbarkeit weder dem Stand der Sicherheitstechnik noch bietet er ausreichend Gewähr, dass über die unterschiedlichsten Anwendungen hinweg keine hoch problematischen Personenprofile erstellt werden.

Biometrie - der Körper kein Schlüssel für Verbrauchergeschäfte

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 (siehe Fingerprint, Augenscan & Co | Arbeiterkammer Wien). 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.

BAK-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 hohen 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 aber erst so 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. Da Anbieter oft mehr um ihren Schutz als den der Kund:innen besorgt sind, braucht es Verbraucherschutzvorschriften, wann und in welcher sicheren Form Identitätsprüfungen erlaubt sind.

BAK-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. Ob elektronischer Führerschein, Buchung eines Mietwagens oder der Kauf von Alkohol: Das als Konkurrenzmodell zu Apple, Google und Co gedachte EU-Vorhaben stößt auf massive Kritik: Eine Verbraucher:innen (Bürger:innen) permanent zugewiesene Kennung ist strikt abzulehnen. Denn sie ermöglicht lebenslanges Profiling über den Einsatz der E-ID bei allen nur denkbaren kommerziellen und behördlichen Kontakten. Digitale Fairness bedeutet: bereichspezifische Abgrenzungen und neu zu generierende Kennungen bei jedem Einsatz der E-ID.

E-Governance nicht ohne digitale Souveränität

Das Daten-Governance Gesetz regelt die kommerzielle Weiternutzung von Daten des öffentlichen Sektors, die aufgrund des Datenschutzes vor dem Zugriff Dritter eigentlich geschützt sind. Er enthält Anmelderegeln für Unternehmen, die Daten gemeinsam nutzen wollen, für Datenvermittler, die als Treuhänder zwischen Privatpersonen und Datennutzern zwischengeschaltet sind und für Organisationen, die „gespendete“ Daten „zum Wohl der Allgemeinheit“ sammeln. Angesprochen sind dabei Daten mit und ohne Personenbezug und solche, bei denen der Personenbezug entfernt wurde, die also anonymisiert wurden. Bezüglich letzterer Kategorie räumen Expert:innen ein, dass Algorithmen durch fortschreitendes maschinelles Lernen so gut wie jede Anonymisierung rückführen können.

Mit anderen Worten: Konsument:innen werden re-identifizierbar. Wann Daten als nicht rückführbar anonymisiert gelten, ist derzeit gesetzlich nicht geregelt.

BAK-Anliegen:

- Bevor persönliche oder pseudonymisierte Daten, die sich im Besitz öffentlicher Stellen befinden, an Unternehmen weitergegeben werden, sind Betroffene von der öffentlichen Stelle darüber zu informieren.
- Digitale Fairness setzt voraus, dass nur anonymisierte Daten die Behördenschnittstelle verlassen und Datennutzer erst nach der Anonymisierung darauf zugreifen können. Werden pseudonymisierte Daten benötigt, ist die Zustimmung der Betroffenen einzuholen (bei erheblichem öffentlichem Interesse können Datenschutzbehörden Genehmigungen erteilen, die Einzelzustimmungen ersetzen).
- Datentreuhänder sind präziser zu regeln, um bei Vertragsstreitigkeiten Rechtssicherheit zu haben, mit welchen Mindestleistungen, Gewährleistungs- und Schadenersatzansprüchen Verbraucher:innen rechnen dürfen.

Autorin: Mag Daniela Zimmer

GERECHTIGKEIT #FÜRDICH

Gesellschaftskritische Wissenschaft: die Studien der AK Wien

Alle Studien zum Download:
wien.arbeiterkammer.at/service/studien