Daniela Zimmer

ANALYSE DES VO-ENTWURFES KÜNSTLICHER INTELLIGENZ AUS VERBRAUCHERSICHT

Juni 2021

WIEN

GERECHTIGKEIT MUSS SEIN

Analyse des VO-Entwurfes Künstlicher Intelligenz aus Verbrauchersicht

Die Absicherung eines hohen Verbraucherschutzniveaus ist uns bei allen Anwendungen, die auf Algorithmen bzw künstlicher Intelligenz (KI) beruhen und mit denen KonsumentInnen in Berührung kommen, ein besonderes Anliegen. Wir setzen uns mit besonderem Nachdruck dafür ein, dass **KonsumentInnen vor einer Aushöhlung ihrer Grund- und Freiheitsrechte, Intransparenz, Diskriminierung und sonstigen Schadensrisiken, die von derartiger Analysesoftware ausgehen,** bestmöglich geschützt werden.

Kurze zusammenfassende Bewertung des Entwurfes aus KonsumentInnensicht:

Um Betroffene angemessen zu schützen, ist erforderlich

- **nicht nur für hochriskante KI Regeln einzuführen**. Ein abgestufter, verpflichtender Rechtsrahmen ist für alle KI-Risikoklassen nötig. Freiwillige Selbstverpflichtungen sind ungeeignet, um Verbraucherrechte zu schützen und Vertrauen zu stärken. Auch bei „bloß“ riskanten Anwendungen in Bezug auf Grund-, Persönlichkeits- und Verbraucherrechte, Schutz von Eigentumsrechten etc sind Transparenz, Diskriminierungsfreiheit, Beschwerderechte durch Vorschriften abzusichern.
- **Rechte für betroffene BürgerInnen und VerbraucherInnen zu verankern**, deren Bedürfnisse überhaupt nicht mitgedacht wurden. Dazu zählen ua das Recht auf Information, Auskunft, Selbstbestimmung in Bezug auf die Möglichkeit, KI-Analysen und Entscheidungen basierend auf persönlichen Daten auch abzulehnen, Beschwerderechte.
- **gesellschaftlich unerwünschte KI-Systeme ausnahmslos zu verbieten** statt lückenhafte Verbote nur für wenige Spielarten von Social Scoring, biometrischer Fernüberwachung und Verhaltensmanipulation.
- **die Risiken, die Hersteller und Nutzer ausschließen bzw minimieren müssen, konkret zu benennen.** So finden sich bei der Beschreibung, wann KI als hochriskant gilt, in Artikel 7 zwar Hinweise auf Gefahren für die Sicherheit, Gesundheit und Grundrechte. Dabei ist weder ein allgemeines Diskriminierungsverbot verankert noch genau normiert, in welchem risikofreien bzw behafteten Zustand KI auf den Markt gelangen darf.
- **das Schließen von Schlupflöchern im korrespondierenden Art 22 DSGVO** bezüglich algorithmischer, automatischer Einzelentscheidungen.
- **eine KI-Zertifizierung ausnahmslos durch unabhängige Behörden** (bzw ihnen zurechenbarer Dienstleister) statt bloßer Selbstzertifizierung durch die Hersteller.
- **dass alle KI-Entscheidungen, -Dienste und -Produkte – bei sonstigem Verbot – tatsächlich erklär- und überprüfbar bleiben**, vor allem in Hinblick auf unzulässige Diskriminierung, Benachteiligung, Verhaltensmanipulation oder Betrügereien.
- **Schutznormen für biometrische KI-Analysen bei Verbrauchergeschäften zu verankern.**
- **keine Ausnahmen von der DSGVO für den Dateneinsatz in „KI-Reallaboren“ vorzusehen.**
- **eine institutionelle Einbindung der Betroffenen** bei interessensabwägenden Entscheidungen über die (Un-)Zulässigkeit von konkreten KI-Anwendungen.
- **die unzeitgemäßen Regeln für Produkthaftung und Produktsicherheit** KI-fit zu überarbeiten.
- **kollektive Rechtsschutzmöglichkeiten für Betroffene ua durch Verbandsklagbefugnisse einzuführen.**

Zu den wesentlichen Bestimmungen des geplanten Entwurfs:

Verbraucheranliegen überhaupt nicht mitgedacht:
Unser Leben wird in viel größerem Maß von automatisierten Verfahren beeinflusst, als die Beispiele des Entwurfes illustrieren. Nicht nur Flugverkehr und Finanzmärkte sind auf komplexe Algorithmen angewiesen. Auch KonsumentInnen werden algorithmisch kategorisiert und bewertet bei Krankenversicherungen in Bezug auf ihre Gesundheit, bei Suchanfragen im Internet, für zielgerichtete Onlinewerbung, News- und Filmempfehlungen oder Betrugs- und Missbrauchskontrollen bei Onlinediensten. Die EU-Kommission bagatellisiert die Risiken, wenn sie dafür lediglich eine freiwillige Selbstverpflichtung empfiehlt.
Denn auch bei der Nutzung „smarter" Konsumgüter und digitaler Dienste können sie mit Intransparenz, Grundrechtsverletzungen, Benachteiligung und Verhaltensmanipulation konfrontiert sein. KI kann dazu dienen, das Alltagsverhalten von KonsumentInnen massenhaft zu überwachen, aus bereits anonymisierten Datensätzen Einzelpersonen wiederzuerkennen, als Informationsfilter Meinungsvielfalt und -freiheit zu bedrohen und Personen Prognosen und klassifizierenden Zuordnungen auszusetzen, die sie benachteiligen. Vor diesem Hintergrund muss der Entwurf um Betroffenenrechte erweitert werden.

Zusätzliche Schutznormen, die über das derzeitige EU-Recht in Bezug auf KonsumentInnenschutz, Datenschutz und -sicherheit, Produkthaftung usw hinausgehen, soll es nur für besonders riskante KI geben. Die BAK hält gesetzliche Anforderungen für ausnahmslos alle KI-Anwendungen für angemessen. Diese sollten entsprechend ihrer Gefahrenneigung abgestuft sein. Mit einer Beschränkung auf Hochrisiko-Anwendungen würden wesentliche Bereiche des Verbraucheralltags unreguliert bleiben. Wann überhaupt ein hohes Risiko vorliegt, wird auch nicht rechtssicher festgelegt.

„KI muss vertrauenswürdig sein!"
Die BAK begrüßt das Postulat der EU-Kommission. Für die EU-Kommission liegen Nutzen und Gefahren bei KI dicht beieinander. Sie zählte bereits in ihrem KI-Weißbuch Bedrohungsszenarien (Personenschäden, Missbrauch zu kriminellen Zwecken …) auf. So richtig der Befund, so schwach sind aber die Rechtsinstrumente, die die EU-Kommission gewählt hat. Für Entwickler und Verwender sollen nämlich keine „unverhältnismäßigen Bürden" entstehen, weshalb sich der Entwurf mit hochriskanten Anwendungen befasst. Ein fundamentaler Fehler: Die Grenze zwischen hochriskant und „nur" riskant verläuft unscharf. Für Geschädigte ist es irrelevant, ob ihr Schaden von einer hochriskanten oder bloß risikobehafteten KI herrührt. Sie erwarten sich in jedem Fall staatliche Regulierung in Form von Schadensprävention durch Vorabkontrolle, Transparenz und Beschwerderechten. Dies ist auch mehr als legitim, bedenkt man, dass Menschen auch ohne ihr Wissen oder ihre Zustimmung zu Betroffenen von Analysen, Überwachung und Entscheidungen diverser KI-Anwendungen werden könnten.

Skepsis gegenüber „ethischer" Technik:
Das Kommissions-Ziel „den Weg für ethische Technik zu ebnen" bleibt in einem Entwurf, der viele KI-Formen reiner Branchenselbstregulierung überlässt, ohnehin unerreicht. Aber auch das Ziel, Technik „ethisch" programmieren zu wollen, gerät in die Kritik. Der deutsche Philosoph Richard David Precht (Künstliche Intelligenz und der Sinn des Lebens) übertitelt seine Überlegungen dazu mit den Worten „Vom Irrsinn, Maschinen Ethik einzuprogrammieren". „Künstliche Intelligenz etwa darauf zu programmieren, wie sie sich in ethischen Grenzfällen verhalten soll" sei „ein Angriff auf die Menschenwürde". Unmissverständliche Verbote seien nötig: „Besonders in ethisch sensiblen Bereichen" bestehe „die Gefahr, dass wir den Maschinen sehr weitreichende Handlungsvollmachten übertragen, die sie auf keinen Fall bekommen dürfen".

Das gelte etwa für Überlegungen, selbstfahrende Autos in unausweichlichen Unfallsituationen mit einem Algorithmus auszustatten, sodass sie „von sich aus entscheiden, ob sie lieber eine Oma überfahren oder ein kleines Kind“.

Benötigt werden klare Ge- bzw Verbote:
Prechts Warnungen sind zweifellos pointiert. Er mahnt allerdings rote Linien für absolut unerwünschte KI völlig zu Recht ein. Unmissverständliche Grenzen setzt der Entwurf aber gerade nicht (Verbote, die nur in wenigen spezifischen Fällen greifen; keine Festlegung, mit welchen maximalen Restrisiken KI auf den Markt geworfen werden darf; kein Verbot von allgemeinen Diskriminierungsrisiken; überwiegende Selbstzertifizierung der Hersteller ohne klare Vorgaben). Es bleibt in hohem Maße den sich selbst zertifizierenden Hersteller und allenfalls noch den nachprüfenden Behörden und Gerichten überlassen, was sie als unannehmbar oder hochriskant und mit flankierenden Maßnahmen tolerabel einstufen.
Der Entwurf sollte demgegenüber Schutz in allen Lebensbereichen, in denen der Einsatz von KI denkbar ist, gewährleisten. Dazu zählen: Verbote ohne vielfältige Ausnahmen, Risikobenennung unter Einbeziehung der Diskriminierungsgefahren, Selbstbestimmungsrechte darüber, ob KI die eigene Person betreffende Entscheidungen überhaupt treffen darf, Informationspflichten, behördliche Vorabprüfung der Folgen für Menschenwürde und Freiheitsrechte, Produktsicherheit und -haftung, außergerichtliche Beschwerdestellen und Verbandsklagsbefugnisse im Interesse aller Betroffenen. Ein bloßer Verweis auf die in Art 22 DSGVO enthaltenen Recht reicht aufgrund dessen Unzulänglichkeiten keinesfalls (siehe https://www.arbeiterkammer.at/interessenvertretung/wirtschaft/konsument/AK-Stn_zur_Evaluation_der_Datenschutz-Grundverordnung.pdf).

Blackbox auch für die Verantwortlichen:
KI ähnelt einer Blackbox, bei der Dateneinsatz, Logik und Entscheidungen für KonsumentInnen intransparent und unverständlich bleiben. Sogar KI-ExpertInnen räumen ein, dass sie sich die Ergebnisse selbstlernender Software selbst nicht erklären können. Wie mit den faktischen Grenzen von Transparenz, Nachvollziehbarkeit und Verantwortung beim Einsatz von selbstlernender KI umzugehen ist, lässt der Entwurf offen. Aus BAK-Sicht gilt: können Hersteller und Nutzer KI-Ergebnisse nicht verantworten, weil sie sie selbst nicht begreifen und beherrschen können, ist die Anwendung zu verbieten.

Transparenz? Jedenfalls nicht für BürgerInnen und VerbraucherInnen:
Informationsrechte sind für „User“ vorgesehen. Damit sind nur die kommerziellen Anwender von KI-Produkten gemeint. Eine Transparenzvorschrift gegenüber Betroffenen ist für einen einzigen Sonderfall vorgesehen: den Gesprächspartnern von Chatbots ist offen zu legen, dass sie mit einem KI-System kommunizieren. Wie sollen sich Betroffene aber erfolgreich dagegen wehren, wenn sie gar keine Kenntnis davon haben, dass eine KI-Anwendung ihre Interessen berührt? Die DSGVO schützt ihre Interessen nur äußerst lückenhaft: Sie sieht Inforechte ausschließlich bei vollautomatisierten Einzelentscheidungen mit rechtlichen (oder ähnlich schwerwiegenden) Folgen für den Betroffenen vor. Sind keine personenbezogenen Daten im Spiel, sind die erwartbaren Folgen (angeblich) nicht rechtlicher Natur, oder arbeitet KI nicht vollautomatisiert, sondern unter menschlicher Aufsicht, so greift die DSGVO und ihre Informations- und Auskunftspflichten nicht. Wer bspw mit anonymisierten/pseudonymisierten Daten ungefragt einer statistischen Gruppe zugeordnet wird, wird davon nicht in Kenntnis gesetzt. Befasst sich vor einer Entscheidung noch ein Mensch mit dem KI-Resultat, so hat der Betroffene ebenso wenig Anspruch darauf, davon zu erfahren. Wer nicht weiß, wo und wie KI-Systemen eingesetzt werden, kann auch nicht abschätzen, ob und wie er/sie davon betroffen ist.

Komplett fehlender Rechtsschutz:
Komplexe Algorithmen und maschinelle Selbstlernfähigkeit werden die zuständigen Aufsichtsbehörden und Gerichte weit über ihre Grenzen fordern. Sie müssten sich idealerweise untereinander abstimmen, um festzustellen, ob Datenschutz, Menschenwürde bzw Persönlichkeitsrechte, Diskriminierungsfreiheit, Produktsicherheit und KonsumentInnenrechte eingehalten werden.

Außergerichtliche Anlaufstellen für Betroffene va auch bei grenzüberschreitenden Problemen:
Es braucht niedrigschwellige Rechtsschutzmechanismen für Betroffene, die die persönlichen Auswirkungen von KI-Entscheidungen kritisch hinterfragen und bekämpfen wollen.
Angesichts der Anerkennung von in einem Mitgliedstaat getroffenen Konformitätsentscheidungen durch andere Mitgliedstaaten, werden VerbraucherInnen regelmäßig Anwendungen ausgesetzt sein, die anderswo und für sie im Detail noch weniger nachvollziehbar zugelassen wurden. Fallen die Niederlassungs- bzw Wohnsitzstaaten von Hersteller, Nutzer bzw dem/der Betroffenen auseinander, so brauchen Letztere kompetente Hilfestellung, um auch grenzüberschreitend Informationen zu KI, die sie betrifft, einfordern oder Beschwerden dazu einbringen zu können.

Mehr Prävention:
KonsumentInnen erwarten sich Vorbeugung durch behördliche Vorabkontrollen und Genehmigungen (statt bloßer Selbstzertifizierung durch die Hersteller und Anwender von KI und nachträglicher Schadenersatzansprüche).

Ohne bestausgestattete Vollzugsbehörden kein Durchblick:
Eine wirksame Marktaufsicht erfordert massive Investitionen in Ressourcen, ohne die Behörden den komplexen Prüfaufgaben weder finanziell noch fachlich gewachsen wären.

Rechtsdurchsetzung im Kollektivinteresse von Betroffenen auf Unterlassung oder Schadenersatz ermöglichen (Beschwerden bei Behörden, Verbandsklagen):
KI geht mit einem hohen Diskriminierungsrisiko gesellschaftlicher Gruppen einher. Es braucht daher auch die Befugnis für Verbraucherverbände und andere NGOs, im kollektiven Interesse einen Anwendungsstopp zu erreichen. Mit individuellen, zivilrechtlichen Schadenersatzansprüchen allein wird kein angemessenes Kräftegleichgewicht zwischen Herstellern bzw AnwenderInnen von KI und den davon nachteilig Betroffenen hergestellt – benötigt werden Verbandsklagsbefugnisse für Organisationen, die VerbraucherInneninteressen vertreten.

Unabhängige Zertifizierung statt dem Motto „der Geprüfte prüft sich überwiegend selbst“: eine externe Zertifizierung durch „notified bodies“ dürfte selbst bei KI-Systemen mit hohem Risiko nur in den seltensten Fällen erfolgen:

- Stand alone - Systeme mit hohem Risiko sind (mit Ausnahme von Punkt 1 des Annex III) bloß einer herstellerinternen Prüfung zu unterziehen.
- KI-Systeme, die in den Annex II fallen, sind gem Art 6 Abs 1 nur dann als KI mit hohem Risiko zu qualifizieren, wenn sie einer externen Zertifizierung unterliegen. Ob dies der Fall ist, entscheiden die „New Approach“-Richtlinien, die die jeweiligen Produktstandards festlegen.
- Diese sehen eine ex ante externe Prüfung durch Zertifizierungsstellen nur ausnahmsweise vor. Bei hochriskanter KI müssten aus BAK-Sicht natürlich ausnahmslos unabhängige, externe Prüfer, herangezogen werden.

Zu den Konsumentenanliegen im Detail:

Zu Art 2 Abs 1 c - Anwendungsbereich
Begrüßt wird, dass auch Hersteller und Nutzer von KI-Systemen aus Drittstaaten vom Anwendungsbereich erfasst sind, sofern die KI-Ergebnisse in der EU **genutzt** werden. Zudem sollte aber in den Anwendungsbereich fallen, wenn EU-BürgerInnen von KI aus Drittstaaten **betroffen** sind.

Zu Art 3 – Definitionen
Die augenfälligen Definitionsdefizite verweisen auf eine Regelungslücke im gesamten Entwurf: Auf von KI betroffene KonsumentInnen und ihren Schutzbedarf wird überhaupt nicht eingegangen.
So sind bspw **„User"** definitionsgemäß nur die professionellen Anwender von KI. Keinerlei Erwähnung finden hingegen die **EndnutzerInnen** (bspw von smarten Produkten, deren Betriebsdaten von KI ausgewertet werden oder digitalen Diensten mit KI-Komponenten).
Dieses Versäumnis ist unbedingt zu beseitigen. Sie sind in den Adressatenkreis unbedingt aufzunehmen, damit auch Schutznormen zu ihren Gunsten verankert werden können.

Bezüglich der Aufnahme des Begriffes der **„Betroffenen"** wird im Übrigen vorgeschlagen: Im Falle der Verwendung personenbezogener Daten für automatische Einzelentscheidungen kann auf die Definition der DSGVO verwiesen werden. Die Betroffeneneigenschaft geht aber weit über den Anwendungsbereich des Artikel 22 DSGVO hinaus. Sie muss sich zB auch auf die KI-basierte Bildung von statistischen Gruppen erstrecken, da auch diese Folgen für die Einzelperson haben kann.

Ziffer 14 definiert die **„Sicherheitskomponente eines Produktes oder Systems".** Warum gerade diese Funktion von KI hervorgestrichen wird, andere aber nicht, wird nicht erklärt. Als Komponente eines Produktes kann KI auch andere (hoch)riskante Funktionen erfüllen (etwa Spracherkennung und Ergebnisauswurf bei Sprachassistenten, biometrische Personenidentifikation bzw Zugangskontrolle bei Handys uvm).

Ziffer 34 definiert **„Emotionserkennungssystem"** als KI-System für Zwecke der Analyse von Emotionen oder Absichten einer Person auf Basis ihrer biometrischen Merkmale. Eine kritische Distanzierung von einem solchen ausnahmslos die Menschenwürde verletzenden Anwendungsgebiet ist weder den Definitionen noch den weiteren Bestimmungen zu entnehmen. Eine klare Abgrenzung zwischen KI-Anwendungen, die grundsätzlich zum Einsatz kommen dürfen und solchen, denen der Betrieb (von wenigen Ausnahmen abgesehen) regelmäßig zu versagen ist, wäre wünschenswert. Ähnlich verhält es sich mit Ziffer 36 (**biometrische Fernidentifikation von Personen**). Auch dieses Einsatzgebiet sollte unter dem Begriff „die Menschenwürde verletzende Anwendungen" rangieren.

Ziffer 44 fasst unter dem Begriff „**ernster Vorfall"** den Tod einer Person, ernste Gesundheitsfolgen oder Schäden am Eigentum, an der Umwelt oder kritischen Infrastrukturen zusammen. Bei der Umschreibung von hochriskanter KI in Artikel 6 ff fehlen einige dieser Tatbestandelemente. Erwähnt werden nur die Gefahr für Gesundheit und Sicherheit, dafür aber werden auch negative Folgen für die Grundrechte erwähnt. Die Risikoszenarien sollten durchgängig kohärent sein.

Zu Art 5 - Verbotene Praktiken
Bei der Präsentation des Entwurfes nahm die EU-Kommission eine strikte Haltung in Bezug auf „unannehmbare Risiken" ein: „KI-Systeme, die als klare Bedrohung für die Sicherheit, die Lebensgrundlagen und die Rechte der Menschen gelten, werden verboten.

Dazu gehören KI-Systeme oder -Anwendungen, die menschliches Verhalten manipulieren, um den freien Willen der NutzerInnen zu umgehen (zB Spielzeug mit Sprachassistent, das Minderjährige zu gefährlichem Verhalten ermuntert), sowie Systeme, die den Behörden eine Bewertung des sozialen Verhaltens (Social Scoring) ermöglichen".
Tatsächlich finden sich im Entwurf unter der Überschrift „Verbotene KI-Praktiken" zwar Praktiken, die in einer auf Grund- und Freiheitsrechten aufgebauten Demokratie tatsächlich überhaupt keinen Platz haben. Ein genauerer Blick zeigt aber: mit ausnahmslosen Verboten ist es nicht weit her. Es werden derart viele Bedingungen, Einschränkungen und Ausnahmen aufgezählt, dass überhaupt kein verlässlicher Schutz vor vielen Spielarten von Manipulation oder Überwachung besteht. Die BAK erinnert an die Leitziele: KI soll „wertebasiert" und „zum ausschließlichen Nutzen der Menschen" eingesetzt werden.

Ziffer a verbietet subliminare, verhaltensmanipulierende Techniken, sofern sie den Betroffenen nicht bewusst sind und physischen oder psychischen Schaden anrichten können. Zum einen fehlt die Erwähnung von wirtschaftlichen Schäden. Zum anderen sollte das Verbot erst gar nicht den Nachweis von Schäden (bzw Eintrittswahrscheinlichkeiten) voraussetzen. Im Werbebereich sind subliminare Techniken auch per se verboten.

Die unbewusste Manipulation von menschlichem Verhalten weist allein für sich hinreichend Unrechtsgehalt auf und ist mit Persönlichkeitsrechten und der Menschenwürde unvereinbar. Auch allgemein bekannte Verhaltensmanipulationen fallen nicht in die von der EU-Kommission postulierte Kategorie einer „werteorientierten KI zum Nutzen der Menschen".

Ziffer b verbietet Techniken, die die Verletzlichkeit bestimmter Personengruppen ausnützen (aufgrund ihres Alters, mentaler oder körperlicher Einschränkungen), um ihr Verhalten zu beeinflussen und daraus (wahrscheinlich) physischer oder psychischer Schaden resultiert. Auch hier darf die Eintrittswahrscheinlichkeit von Schäden doch nicht ernsthaft eine Voraussetzung für ein Verbot sein. Die Verletzlichkeit von besonders geschwächten Menschen manipulativ auszubeuten, stellt in einer demokratischen Ordnung, die auf Fürsorge für Schwächere aufbaut, ein per se verpöntes Verhalten dar – völlig unabhängig von einem Schaden.

Ziffer c verbietet „social scoring", wie EG 17 die behördliche Absicht umschreibt, die „Vertrauenswürdigkeit" von Personen anhand ihres „sozialen Verhaltens" zu bewerten. Die Bestimmung hat sichtlich das chinesische Experiment, die Bevölkerung nach politisch und sozial (un-)erwünschtem Verhalten (aus) zu sortieren, vor Augen. Viele Spielarten von grundrechtswidrigem Scoring wären dennoch erlaubt. Verboten wird nämlich nur soziales Scoring, das auf Daten basiert, die ursprünglich für andere Zwecke gesammelt wurden oder im Falle von Benachteiligungen, die gemessen am sozialen (Fehl-)Verhalten unverhältnismäßig sind. Mit anderen Worten: stünden für KI Daten zur Verfügung, die originär für Zwecke des Scorings gesammelt wurden, wäre dies aus Sicht der EU-Kommission offenbar unproblematisch. Sogar Benachteiligungen von Personen wären statthaft, solange sie im Vergleich zum sozialen (Fehl-)Verhalten der Person nicht unverhältnismäßig sind.

Welche Behörde darf sich in einer demokratischen Ordnung überhaupt anmaßen, personenbezogene Daten in der Absicht zu sammeln, die Vertrauenswürdigkeit und das Sozialverhalten seiner BürgerInnen numerisch zu bewerten? Derartige Vorhaben berühren rasch die Menschenwürde, weshalb es kaum Spielraum für zulässige Anwendungen gibt. Wir dürfen an dieser Stelle an einen Meilenstein der Grundrechtsjudikatur, das deutsche „Volkszählungsurteil" aus 1983 erinnern**:** „Mit dem Recht auf informationelle Selbstbestimmung wären eine Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.

Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."

Benötigt wird daher ein generelles Verbot der sozialen Überwachung und Profilbildung der Bevölkerung. Alle Abwägungen müssten andernfalls Einzelfallsentscheidungen der Gerichte überlassen werden. Was lässt sich bspw unter „Vertrauenswürdigkeit über einen gewissen Zeitraum basierend auf Sozialverhalten" subsumieren? Was sind „persönliche Charakteristiken", „Charakteristiken der Persönlichkeit" oder „nachteilige Behandlungen im sozialen Kontext"?
Unklar ist auch, was für social scoring gilt, das vom extrem lückenhaften Verbot nicht erfasst und dennoch grundrechtswidrig ist. Warum sind nur Behördenpraktiken erfasst, aber nicht auch jene von Unternehmen, die Personen in jeder denkbaren Richtung „scoren" (möchten)? Unter welchen Umständen ist Unternehmen bspw die Vorbeugung bzw Aufdeckung von Betrug und Missbrauch mittels social scores erlaubt bzw untersagt? Das latente Misstrauen gegenüber KonsumentInnen in Bezug auf die Rechtmäßigkeit ihres Verhaltens verletzt den Vertrauensgrundsatz in einem Rechtstaat und führt zu einer äußerst undemokratischen Absicherungsgesellschaft, die Konsumentenverhalten auf Schritt und Tritt durch Datensammlungen und deren algorithmische Auswertung überwacht und bewertet.

Warum sind gerade Datenanalysen rund um die „Vertrauenswürdigkeit" einer Person erfasst, nicht aber andere, die Persönlichkeitsrechte gleichermaßen tief verletzen können (Vorlieben, Emotionen, Gesundheit, Intelligenz, Leistungskraft uvm)? Können Praktiken, die nach Art 5 nicht untersagt sind, mit Blick auf die EMRK oder Art 22 DSGVO verboten werden? (etwa soziales Scoring durch die Privatwirtschaft oder Bewertungen von anderen Eigenschaften als der „Vertrauenswürdigkeit" einer Person). Der Entwurf böte jedenfalls die Chance, auch Unzulänglichkeiten im Artikel 22 DSGVO zu beseitigen (Erweiterung des Schutzes auf statistische Gruppen, bei denen kein Personenbezug vorliegt und auf Fälle mit abschließender menschlicher kontrollierender Aufsicht). Auch die Ausnahmen vom Verbot (Einwilligung, Rechtsakt, Vertragsnotwendigkeit) sind zu weitreichend und deshalb überarbeitungsbedürftig (siehe dazu die Vorschläge der BAK unter https://www.arbeiterkammer.at/interessenvertretung/wirtschaft/konsument/AK-Stn_zur_Evaluation_der_Datenschutz-Grundverordnung.pdf).

Ziffer d verbietet die biometrische Fernidentifikation von Personen in Echtzeit im öffentlichen Raum für Zwecke der Rechtsdurchsetzung. Auch hier gibt es umfangreiche Ausnahmen: die zielgerichtete Suche nach „potentiellen" Verbrechensopfern, die Vorbeugung der Lebensbedrohung von Personen oder von terroristischen Attacken und die Aufdeckung, Lokalisierung, Identifikation oder Verfolgung von Personen, die eines schweren Verbrechens (Strafrahmen 3 Jahre) verdächtigt werden. Sehr begrüßt wird, dass der Einsatz solcher biometrischen Systeme in der Regel (Ausnahmen bei Gefahr in Verzug) einer vorherigen Genehmigung durch die Justiz oder einer unabhängigen Verwaltungsbehörde bedarf.

Angemessen wäre allerdings auch hier ein weitgehend ausnahmsloses Verbot des Einsatzes KI-basierter biometrischer Erkennung von Personen ohne deren Zustimmung (unabhängig von Echtzeit- und Remote-Erfassungen).
Unvertretbar erscheint uns bspw die Einschränkung auf Echtzeiterfassungen. Auch die biometrische Auswertung von Videomaterial kann tief in Grundrechte eingreifen. Wir verweisen beispielshaft auf die medial bekannt gewordenen Skandalfälle PimEyes (polnische KI-Anwendung) und Clearview (US-KI-Anwendung), die Milliarden Profilfotos im Internet mittels KI auswerteten und die Identitätsdaten verkauften.

Auch die Reichweite der Erlaubnistatbestände ist zu groß: letztlich kann jede/r „potentielles“ Opfer eines Verbrechens werden. Auch die Maßgaben in Abs 2 (Wahrscheinlichkeit bzw Ausmaß des Schadens und Folgen für Betroffene sind in Betracht zu ziehen) schützen nicht vor Massenüberwachung: Wenn auf einem Platz in der Vergangenheit immer wieder Personen überfallen wurden und nun massenhaft Passanten biometrisch überwacht würden, wäre der Kollateralschaden der anlasslos mitüberwachten Passanten entscheidungsrelevant oder dass alle Passanten auch als denkmögliche, potentielle Opfer durch die Maßnahme geschützt werden?

Wir erinnern daran, dass Arbeitspapiere der EU-Kommission ein mehrjähriges Verbot der KI-Analyse von biometrischen Merkmale für private wie öffentliche Akteure enthielten. Denn zwischenzeitig sollte eine „solide Methodologie für die Einschätzung der Folgen der Technologie und mögliche Risikomanagementmaßnahmen“ entwickelt werden. Für den Grundrechtsschutz in der EU ist es das falsche Signal, wenn der Entwurf kein (zumindest temporäres) Einsatzverbot ausspricht. Die Technologie wirft massive datenschutzrechtliche Bedenken auf, die auch von Organisationen wie Privacy International oder Bits of Freedom ausführlich dargestellt worden sind. Eine Fehlerrate von 1 % bedeutet etwa: Sind 10.000 Menschen einer Gesichtserkennung ausgesetzt, die polizeilich gar nicht gesucht werden, dann werden 100 von ihnen dennoch als gesucht markiert. Ein Test, der 2018 in London durchgeführt wurde, ergab 104 Übereinstimmungen, von denen nur zwei richtig waren – alle anderen waren Falsch-Positive.

Da alle unsere KonsumentInnenanliegen in Bezug auf Biometrie den Rahmen dieser Stellungnahme sprengen würden, verweisen wir auf unsere gemeinsam mit der Akademie der Wissenschaften erstellte Studie „Fingerprint, Augenscan und Co – der digitale Kontrollverlust“ abrufbar unter Fingerprint, Augenscan & Co | Arbeiterkammer Wien. Unsere Regulierungsanliegen:

- **Biometrie darf kein Geschäft werden:** Dier Handel mit biometrischen Daten und die Weitergabe an externe Dritte sollte verboten und mit hohen Strafen sanktioniert sein.
- **Wahlfreiheit ist oberstes Gebot:** Jede/r 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.
- **Onlinebanking und andere Anwendungen ohne bleibende biometrische Daten:** Es darf zu keiner dauerhaften Speicherung von biometrischen Daten oder deren digitaler Komponenten (Hashwerte, etc) kommen, um das Risiko von Identitätsdiebstahl zu minimieren.
- **Gesichtsfotos als sensible Daten:** Onlinefotos mit Gesichtern werden bereits in unzähligen Fällen für die Identifikation von Personen durch Gesichtserkennung genutzt. Rechtlich ist offen, inwieweit diese Daten als biometrisch gelten. Hier besteht dringendster Bedarf, Porträtbilder vor versteckter biometrischer Auswertung zu schützen.

Zu Art 6 Abs 1 – Klassifizierung von KI-Systemen als hoch-riskant

Hochriskant sind KI-Systeme nur dann, wenn sie als Sicherheitskomponente oder - produkt nach den in Anhang II angeführten Harmonisierungsrechtsvorschriften gelten. Zusätzlich muss die Sicherheitskomponente bzw das Sicherheitsprodukt einer Konformitätsbewertung durch Dritte wiederum nach den in Anhang II angeführten Harmonisierungsrechtsvorschriften unterzogen werden.
KI wäre nur dann hochriskant, wenn sie mit einer externen Zertifizierung nach den „New Approach“ RL über die technische Produktkonformität verbunden ist. Für die Qualifizierung eines KI-Sicherheitsproduktes als hochriskant kann aber nicht ernsthaft ausschlaggebend sein, ob es einer New Approach RL unterliegt und nach dieser extern zu zertifizieren ist (was im Übrigen selten der Fall ist). Dieser Ansatz ist verfehlt und muss durch sachgerechte Kriterien ersetzt werden.

Zu Art 6 Abs 2 iVm Annex 3 und Art 7
Als hochriskant gelten zudem die im Annex 3 aufgezählten Anwendungen. Diese Liste sollte nur deskriptiv sein, denn wichtige Bereiche finden gar keine Erwähnung (zB KI, die sensible Gesundheitsdaten benutzt, Betrugs- und Missbrauchserkennung aufgrund des Kundenverhaltens, werblich-manipulative Beeinflussung des Nutzerverhaltens etwa durch individuelle Preisanpassung, Produktempfehlungen, Nachrichtenselektion uvm).

Nach Art 7 Abs 1 kann die EU-Kommission Annex III auch ergänzen. Sie darf allerdings nur die bereits angelegten Kategorien (zB Biometrie, Strafverfolgung etc) um weitere Beispiele erweitern. Neue Kategorien sind ausgeschlossen. Damit können wichtige, verbraucherrelevante Bereiche nicht erfasst werden. Zudem muss von weiteren Beispielen ein hohes Risiko in Form von Schäden an Gesundheit oder Sicherheit oder eine negative Beeinträchtigung von Grundrechten ausgehen. Auch wirtschaftliche Schäden sind zu erwähnen.

Zum Annex:

- Die Erfassung von „**KI-Systemen, die für die biometrische Echtzeit-Fernidentifizierung** und nachträgliche biometrische Fernidentifizierung natürlicher Personen verwendet werden sollen“ ist zu eng. Wie auch schon bei Artikel 5 ausgeführt sind biometrische KI-Systeme auch bei Verbrauchergeschäften im Vormarsch (Onlinebanking, Geräteentsperrung, Altersverifikation), bei denen keine „Fern“-Identifikation stattfindet. Aufgrund der eminent hohen Missbrauchsgefahr und den beträchtlichen Fehlerraten sollten auch diese Anwendungen mitreguliert werden.

- Bei der „**Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen**“ bedarf es erläuternder Beispiele, was in die Kategorie „grundlegende private Diensten“ fällt.

- Die „**Kleinanbieter-Ausnahme für den Eigengebrauch**“ in Bezug auf „KI-Systeme, die für die **Kreditwürdigkeitsprüfung und Kreditpunktebewertung** natürlicher Personen verwendet werden sollen“ sollte kritisch hinterfragt werden. Risiken bestehen unabhängig von der Unternehmensgröße.

- „**KI-Systeme, die von Strafverfolgungsbehörden für individuelle Risikobewertungen** natürlicher Personen verwendet werden sollen, um das Risiko abzuschätzen, dass eine natürliche Person Straftaten begeht oder erneut begeht…“ sollten zu den absolut verbotenen Praktiken des Artikel 5 zählen. Die damit regelmäßig einhergehende Verletzung der Menschenwürde, die hohen Fehlerraten, diskriminierenden Bias uvm sind nur einige der Gründe, warum innerhalb der EU für derartige Anwendungen grundsätzlich kein Platz sein sollte. Auch „KI-Systeme, die von Strafverfolgungsbehörden **als Lügendetektoren** und ähnliche Instrumente oder zur Ermittlung des emotionalen Zustands einer natürlichen Person verwendet werden sollen“ sollten der Liste verbotener Praktiken hinzugefügt werden. Nicht nur als hochriskant, sondern in einer Demokratie als unannehmbar sollten außerdem KI-Systeme gelten, “die von Strafverfolgungsbehörden **zur Vorhersage des Auftretens einer tatsächlichen oder potenziellen Straftat auf der Grundlage des Profils natürlicher Personen** oder zur Bewertung von Persönlichkeitsmerkmalen und Eigenschaften oder vergangenen kriminellen Verhaltens natürlicher Personen oder von Gruppen verwendet werden sollen.“ Außerdem sind KI-Systeme, „die zur Kriminalanalyse natürlicher Personen eingesetzt werden sollen und es den Strafverfolgungsbehörden ermöglichen, große **komplexe verknüpfte und unverknüpfte Datensätze aus verschiedenen Datenquellen** oder in verschiedenen Datenformaten zu durchsuchen, **um unbekannte Muster zu erkennen oder verdeckte Beziehungen in den Daten aufzudecken**“ mit den Grundregeln des Datenschutzes unvereinbar und deshalb verboten.

Artikel 13 - Transparenz und Bereitstellung von Informationen für die Nutzer
Es ist unakzeptabel, dass nur dem professionellen Anwender („Nutzer“) Infos zum KI-Betrieb zugänglich sein müssen. Auch Betroffene haben einen Anspruch auf Transparenz (die Informationspflichten der DSGVO erstrecken sich nicht auf alle Formen von KI). Die in Abs 3 genannten Informationen (den Namen und die Kontaktangaben des Anbieters, die Merkmale, Fähigkeiten und Leistungsgrenzen des KI-Systems, einschließlich seiner Zweckbestimmung, des Maßes an Genauigkeit, Robustheit und Cybersicherheit, alle bekannten oder vorhersehbaren Umstände im Zusammenhang mit der bestimmungsgemäßen Verwendung des Hochrisiko-KI-Systems oder einer vernünftigerweise vorhersehbaren Fehlanwendung, die zu Risiken für die Gesundheit und Sicherheit oder die Grundrechte führen können, Informationen über die verwendeten Testdatensätze…) müssen daher auch den von der Anwendung Betroffenen zugänglich sein.

Zu Art 14 – menschliche Aufsicht
Die Anforderung einer menschlichen Aufsicht wird begrüßt. Unklar ist, welche Qualitätsanforderungen dabei einzuhalten sind. Unklar ist auch, in welchem Verhältnis diese Anforderung zu Artikel 22 DSGVO steht, der automatisierte Einzelentscheidungen grundsätzlich auch ohne menschliche Aufsicht gestattet, dem Betroffenen allerdings das „Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunktes und auf Anfechtung der Entscheidung“ einräumt.

Zu Art 17 – Qualitätsmanagement
Abs 1 (a) verpflichtet den Provider zu einer Strategie ua für die rechtliche Konformität. Es sollte klargestellt werden, dass diese auch die Einhaltung der datenschutzrechtlichen Bestimmungen umfasst. Nach Abs 2 sollen die Verpflichtungen nach Abs 1 sich nach der Größe des Unternehmens richten. Dies ist abzulehnen: Risiken müssen jedenfalls unabhängig von der Unternehmensgröße mit größter Sorgfalt minimiert werden.

Zu Art 47 – Aussetzung der Konformitätsbewertung
Marktüberwachungsbehörden sollen Verfahren zur Konformitätsbewertung in bestimmten Fällen aussetzen können. Die dafür ausschlaggebenden „außergewöhnlichen Gründe“ sind viel zu unbestimmt.

Zu Art 52 – Transparenzpflichten für bestimmte AI-Systeme
Die (einzigen) Informationspflichten beim Einsatz von Chatbots gegenüber Betroffenen sind grundsätzlich sehr zu begrüßen. Die Bestimmung ist um generelle vorherige Informations- und nachträgliche Auskunftsrechte für alle von KI betroffenen Personen zu erweitern. Emotionserkennungssysteme greifen erheblich in die Grundrechte von Personen ein – eine bloße Kenntlichmachung ist keine hinreichende Schutzmaßnahme. Ihr Einsatz sollte grundsätzlich zu den verbotenen Praktiken des Artikel 5 zählen.

Artikel 54 - Weiterverarbeitung personenbezogener Daten in „KI-Sandboxes/Reallaboren“
In sogenannten KI-Reallaboren sollen personenbezogene Daten, die eigentlich für andere Zwecke erhoben wurden, zum Testen von KI benutzt werden dürfen, wenn ein erhebliches öffentliches Interesse besteht (bei der Verfolgung von Straftaten, bezüglich Gesundheit oder Umwelt) und mit anonymen Daten nicht das Auslangen gefunden werden kann. Diese Bestimmung höhlt aus BAK-Sicht in unakzeptabler Weise die DSGVO aus: der Weiterverarbeitung von Daten für einen anderen Zweck sind durch Artikel 6 Abs 4 DSGVO nämlich enge Grenzen gesetzt. Vor diesem Hintergrund wären die Betroffenen von einem solchen Vorhaben zu informieren und ihre Zustimmung einzuholen. Eine Missachtung des Selbstbestimmungsrechtes der Betroffenen über ihre persönlichen Daten wäre in hohem Maße grundrechtswidrig und läuft auch Gefahr, einer EUGH-Kontrolle nicht standzuhalten.

Zudem sei zu überwachen, ob während des Testens hohe Grundrechtsrisiken bestehen. Auch diesem Risiko kann man Personen aus BAK-Sicht nicht zu Testzwecken ungefragt aussetzen. Es braucht eine explizite Zustimmung, als Proband zur Verfügung zu stehen. Die Datenschutzbehörde hat ein solches Vorhaben außerdem vorab zu prüfen und geeignete Auflagen zu erteilen oder das Vorhaben, soweit es nicht DSGVO-konform durchgeführt werden kann, zu untersagen.

Weitere Verbraucheranliegen:

Hersteller und Nutzer hochriskanter Anwendungen benötigen eine Haftpflichtversicherung:

Es ist klarzustellen, dass beide Unternehmen Betroffenen gegenüber für materielle und immaterielle Schäden solidarisch haften (der Geschädigte kann sich aussuchen, wen er in Anspruch nimmt; im Innenverhältnis ist je nach Verschuldenslage ein Regress möglich). Aufgrund der Gefahr, dass hohe Schadenersatzsummen aus dem Vermögen des Verantwortlichen nicht gedeckt werden können, sollte eine Versicherungspflicht bestehen. Ein öffentlich zugängliches Register soll Auskunft geben, welche Versicherung für die Schadensdeckung aufkommt.

Regeln zugunsten einer leichten Rechtsdurchsetzung fehlen:

Es sind für Betroffene nationale Anlaufstellen einzurichten.
Wenn sie keine aussagekräftigen Vorabinformationen oder Auskünfte auf entsprechendes Verlangen erhalten, sollten sie diese auf diesem Weg einfordern können. Hält der Betroffene KI-Ergebnisse für unrichtig, unsachlich benachteiligend oder anderweitig rechtswidrig, muss er ebenso niedrigschwellig und ohne Kostenrisiko eine Nachprüfung verlangen können. Zur Unterstützung der kollektiven Interessen von Betroffenengruppen auf Unterlassung und Schadenersatz ist eine Verbandsklagsbefugnis und Beschwerdemöglichkeiten bei den zuständigen Behörden vorzusehen. Aufgrund der grenzüberschreitenden Anerkennung von KI sollten die zuständigen Behörden nach dem Konzept der DSGVO Beschwerden aus dem jeweiligen Mitgliedstaat entgegennehmen und an die zuständige Behörde des Niederlassungsstaates weiterleiten.

In der DSGVO müssen Schlupflöcher für den Einsatz intransparenter Algorithmen geschlossen werden

Derzeit sind Artikel 22 der DSGVO zufolge nur vollautomatisierte Einzelentscheidungen, die Rechtsfolgen haben oder KonsumentInnen erheblich beeinträchtigen, grundsätzlich verboten. Der Schutz muss auch auf „halbautomatisierte“ Entscheidungen erweitert werden. Denn Unternehmen wenden oft ein, dass Maschinen nicht selbst entscheiden, sondern menschliche Entscheidungen „nur“ vorbereiten. Maschinelle Bewertungen werden von MitarbeiterInnen (allein des hohen Begründungsaufwands wegen) nachträglich aber kaum mehr abgeändert.
Außerdem sollten Betroffene über jeden Algorithmus, der mit Daten von KonsumentInnen arbeitet, informiert werden – unabhängig von den Rechtsfolgen oder einer starken Beeinträchtigung der KonsumentInnen, wie es die DSGVO derzeit verlangt.
Auch die Erlaubnistatbestände des Artikel 22 gehen viel zu weit: algorithmische Entscheidungen sind etwa zulässig, wenn sie für den Abschluss oder die Erfüllung von Verträgen nötig sind und der betroffene Konsument eine Chance erhält, seinen Standpunkt zu erklären und die Entscheidung anzufechten. Der Einsatz bei Verbraucherverträgen sollte nur in besonders begründeten Fällen (wie einem hohen Zahlungsausfallsrisiko bei Krediten) möglich sein.
Der Einsatz der Technik, die verwendeten Daten und Logik sind für die Betroffenen nach wie vor extrem schlecht nachvollziehbar, denn auch bei Auskunftsersuchen bleibt vieles Geschäftsgeheimnis.

Einbindung der Betroffenen

Daten- und Privatsphärenschutz sollten wirtschaftlichen Interessen grundsätzlich vorgehen. Wie verhält es sich aber, wenn Eingriffe in diese Rechte mit lebenswichtigen Interessen einzelner Personen, von Gruppen oder der Gesamtgesellschaft begründet werden? Interessenskollisionen sind vorprogrammiert, sobald KI-Anwendungen im Gesundheitssektor Verbesserung bei der Erkennung, Behandlung und Heilung von Krankheiten oder im sicherheitspolizeilichen Einsatz eine bessere Kriminalitätsprävention bzw -aufklärung versprechen. Der Preis für diesen (potentiellen) Fortschritt ist hoch: Interessen von großen Bevölkerungsteilen können damit gefährdet werden. Vor diesem Hintergrund braucht es für die Mehrzahl an KI-Anwendungen, die Grundrechte berühren, eine ex ante-Genehmigung durch ein unabhängiges Gremium. In dieses sind neben Datenschutzbehörden und Technikexperten auch Vertreter der jeweils betroffenen Gruppen (ArbeitnehmerInnen, KonsumentInnen, PatientInnen, VerkehrsteilnehmerInnen etc) miteinzubeziehen.

Denn auch bei der Klärung von Rechtsfragen wird sorgfältig zwischen verschiedenen Interessen, Verhältnismäßigkeiten, Werten etc abzuwägen sein. Diese Entscheidungen können abhängig von der jeweiligen Betroffenheit und dem jeweiligen weltanschaulichen Hintergrund sehr verschieden ausfallen. Die gesellschaftliche Akzeptanz von Entscheidungen für oder gegen einzelne KI-Anwendungen und flankierende Auflagen fällt höher aus, wenn bei der Zusammensetzung des Entscheidungsgremiums auf eine breite Beteiligung aller betroffenen Gruppen geachtet wird.

Aber nicht nur im Bereich der Grundrechte wäre eine stärkere Einbindung von Betroffenen sinnvoll. Es hat sich auch gezeigt, dass etwa im Unternehmenskontext die Einführung von KI-Systemen in Produktions- und Organisationsabläufen wesentlich zielgerichteter und besser eingeführt werden können, wenn VertreterInnen von Arbeitnehmern (Betriebsrat und überbetriebliche Interessensvertretungen) frühzeitig eingebunden werden und die Projekte von Anfang an begleiten und mitgestalten können. Auch hier sollte mehr Augenmerk daraufgelegt werden, dies auch aktiv zu fördern.

Der direkte Weg zu unseren Publikationen:
E-Mail: konsumentenpolitik@akwien.at

Impressum

Medieninhaber: Kammer für Arbeiter und Angestellte für Wien,
Prinz-Eugen-Straße 20–22, 1040 Wien, Telefon: (01) 501 65
Offenlegung gem. § 25 MedienG: siehe wien.arbeiterkammer.at/impressum
Zulassungsnummer: AK Wien 02Z34648 M
AuftraggeberInnen: AK Wien, Konsumentenpolitik
Autorin: Daniela Zimmer
Grafik Umschlag und Druck: AK Wien
Verlags- und Herstellungsort: Wien

Stand Juni 2021
Im Auftrag der Kammer für Arbeiter und Angestellte für Wien

Gesellschaftskritische Wissenschaft: die Studien der AK Wien

Alle Studien zum Downloaden:

wien.arbeiterkammer.at/service/studien

AK WIEN