Von personalisierter Werbung zur staatlichen Verfolgung

Zweckbindung als Grundrechtsschutz im Zeitalter von KI

Rainer Mühlhoff & Hannah Ruschemeier

03.02.2026 doi: 10.59704/8d8b05c35e77a462

Die US-amerikanische Immigration and Customs Enforcement Agency (ICE) hat angekündigt, die „AdTech- und Big-Data-Tools" privater Unternehmen für die Verfolgung vermeintlich illegaler Einwanderer nutzen zu wollen. Die Forderung zeigt in schonungsloser Offenheit, wie groß das Missbrauchspotenzial von Geschäftsmodellen ist, die auf massenhafter aggressiver Datenextraktion beruhen. Gepaart mit der ökonomischen Struktur des heutigen Internets und der Realität des Technologie-Oligopols in der Hand weniger Firmen entfaltet sich ein dystopisches Potenzial: Private Datenmacht verbindet sich mit einer Behörde, die über erhebliche Vollzugs- und Zwangsbefugnisse verfügt. Darin zeigt sich eine neue Stufe der Erosion demokratischer Kontrolle und Rechtsstaatlichkeit.

Datenmacht und Vorhersagetechnologien als Risiko

„AdTech" (Advertising Technology) bezeichnet das Geschäftsfeld der Big-Data- und KI-Industrie, in dem digitale Werbung automatisiert ausgespielt, gemessen und optimiert wird. Besser bekannt als „personalisierte Werbung" handelt es sich dabei um eine seit mehr als 20 Jahren gewachsene Industrie, die auf der systematischen und flächendeckenden Sammlung von Tracking- und Verhaltensdaten im Internet beruht. Anhand der Datenspur einer Nutzer:in werden mit statistischen Verfahren Persönlichkeitsmerkmale ermittelt – Bildungsstand, Interessen, psychologische Profile, Krankheitsrisiken, demographische oder sozioökonomische Informationen – anhand derer dann entschieden wird, welche Werbung für diese Nutzer:in am „effizientesten" ausgespielt werden kann.

Solche Modelle lassen sich prinzipiell auf *jede beliebige* Person zur Vorhersage von Informationen anwenden, die diese Person nie irgendwo preisgegeben hat. Dies prägt die erhebliche informationelle Machtakkumulation, die mit AdTech verbunden ist. Seit den 2000er-Jahren ist die Industrie bemüht, das Image zu verbreiten, dass personalisierte Werbung gesellschaftlich harmlos sei. Der potenzielle Zugriff einer Behörde wie ICE auf diese technologischen Machtinstrumente zeigt jedoch das verheerende Missbrauchspotenzial dieser Technologie.

Dieses Missbrauchspotenzial realisiert sich bei der Zweckentfremdung ursprünglich kommerzieller und ziviler Technologie für den behördlichen Vollzug. Darin liegt eine gefährliche Vermischung des staatlichen Gewaltmonopols mit weitgehend unregulierter privater Wirtschaftsmacht. Bei den statistischen Verfahren der AdTech-Industrie handelt es sich um prädiktive Machine-Learning-Systeme, die massenweise Vergleichsdaten benötigen, um trainiert zu werden. Deshalb liegt der AdTech-Markt fest in der Hand weniger großer Plattformunternehmen, die über Milliarden Nutzer:innen und somit über die Möglichkeit der Datenaggregation verfügen – darunter prominent Google, Meta, Apple, Amazon und Microsoft.

Wer also AdTech betreibt, der hat eine ganz besondere Form von *Datenmacht,* die wir Vorhersagemacht nennen. Diese besteht aus informationstechnischen Apparaten, die die Vorhersage nahezu beliebiger Persönlichkeitseigenschaften von Individuen anhand von vergleichsweise leicht erhältlichen Nutzungsdaten (Tracking, Social Media, Apps) erlauben. Der Katalog der Datenpunkte, die große Plattformen routiniert über *alle* ihre Nutzer:innen abschätzen, um sie für personalisierte Werbung zu verwenden, umfasst hunderte geschätzter Attribute, von religiösen Neigun-

gen und ethnischer Herkunft bis zu Substanzmissbrauch, Beziehungsstatus oder politischen Ansichten. Der EuGH hat dazu ausgeführt, dass die Datenverarbeitung von Meta erhebliche Auswirkungen auf Nutzer:innen hat, deren Online-Aktivitäten zum großen Teil, wenn nicht sogar fast vollständig, von Meta aufgezeichnet werden, was bei Nutzer:innen das Gefühl auslösen kann, dass ihr Privatleben kontinuierlich überwacht wird.

ICE, Daten und KI-Technologie

ICE ist eine finanziell überproportional gut ausgestattete Behörde, die dieses Budget auch bisher dazu genutzt hat, unterschiedliche Digitaltechnologien zu erwerben. Wäre ICE eine Armee, läge es auf Platz 14 der bestfinanziertesten Militärs der Welt. Bereits seit einigen Jahren setzt ICE auch auf zunehmend digitale Überwachungstechnologien im alltäglichen Einsatz; die Behörde hat verschiedene Verträge zur Überwachung von Aufenthaltsorten, Gesichtserkennung, Spyware, Social-Media- und Telefonüberwachung abgeschlossen. Um zwei Beispiele aufzugreifen: ICE nutzt Software, die Standortdaten von Millionen von Menschen von Datenhändlern sammelt, um diese mit öffentlichen Social-Media-Daten zu verbinden. Die Firma Penlink verkauft diese Informationen dann an ICE, damit die Behörde ohne eine gerichtliche Entscheidung Kenntnisse über Aufenthaltsorte und Standortdaten erlangen kann. Ein weiteres von ICE genutztes KI-Tool nennt sich Onyx und wurde von der Firma Fivecast entwickelt. Onyx wird beworben als „KI-gestützte Risikoanalyse – alles auf einer Plattform. Sie erhalten Zugriff auf Milliarden von Datenpunkten aus Millionen von Quellen, sodass Sie Bedrohungen schneller und genauer aufdecken können."

Wie in allen anderen Einsatzbereichen auch, sind diese Technologien fehleranfällig. Die von ICE verwendete Gesichtserkennungs-App hat mehrfach Personen falsch identifiziert – Kontrollmechanismen oder Qualitätssicherungsvorgaben sind nicht bekannt, die Grundrechtsrelevanz im Kontext der Entscheidung über eine Abschiebung im Schnellverfahren ist offensichtlich.

Machtmissbrauch durch Zusammenarbeit mit kommerziellen Diensten

Im Zuge der technologischen Hochrüstung von ICE markiert die aktuelle Anfrage an Unternehmen der US-amerikanischen AdTech-Industrie eine neue Eskalationsstufe. Erstmals zielt die Behörde explizit darauf ab, Datenbestände und Vorhersagetechnologien zu nutzen, die für kommerzielle und zivile Zwecke entwickelt wurden. Konkret sollen Modelle zur Vorhersage von Persönlichkeitsmerkmalen, die bislang der Personalisierung von Werbung dienten, zur Identifikation und Verfolgung vermeintlich illegaler Migrant:innen eingesetzt werden.

Da es sich bei den KI-Systemen der AdTech-Industrie um besonders leistungsfähige, mit enormen Datenmengen trainierte Modelle handelt, stellt ihre staatliche Nutzung eine schwerwiegende Bedrohung für Freiheit und Grundrechte dar. Hier verbindet sich eine weitgehend unregulierte private Daten- und Vorhersagemacht mit hoheitlichen Zwangsbefugnissen. Die Zweckentfremdung ziviler Technologien für behördlichen Vollzug offenbart einen grundlegenden Machtmissbrauch und den nächsten Schritt der Erosion rechtsstaatlicher Garantien.

Ein warnendes Beispiel für Europa

Über den konkreten US-amerikanischen Kontext hinaus ist dieser Fall insbesondere aus europäischer Perspektive von Bedeutung. Entscheidend ist nicht allein das Handeln von ICE, sondern das gesellschaftliche und systemische Risiko, das bereits in der bloßen Existenz der zivilen technologischen Infrastruktur der AdTech-Industrie angelegt ist. Die dort stattfindende Akkumulation informationeller Vorhersagemacht birgt inhärent die Gefahr missbräuchlicher Sekundärnutzung und eines schleichenden „function creep".

Um Gesellschaften wirksam vor diesem Risiko zu schützen, muss dieses in einer *präventiven* Herangehensweise als systemisches Risiko analysiert werden. Ohne regulatorische und organisatorische Maßnahmen, die Daten und KI-Modelle dauerhaft an ihren ursprünglichen Verwendungskontext – hier die Personalisierung von Werbung – binden, können solche

mächtigen Werkzeuge in veränderten politischen Konstellationen jederzeit für grundrechtsgefährdende Zwecke eingesetzt werden. Genau in diesem Missbrauchspotenzial, das überall dort entsteht, wo der Einsatz mächtiger Technologien nicht hinreichend begrenzt ist, liegt eine Dimension systemischen Risikos, die in der europäischen Politik bislang weitgehend verkannt wird. Der Fall ICE ist daher nicht nur ein US-amerikanisches Problem, sondern ein warnendes Beispiel dafür, welche Gefahren auch europäischen Rechtsstaaten drohen, wenn Zweckbindung und demokratische Kontrolle datenbasierter Geschäftsmodelle nicht wirksam abgesichert werden.

Zweckbindung als Grundrechtsschutz

Das rechtliche Instrument der Zweckbindung zielt darauf ab, genau solche Missbrauchsgefahren von Datenmacht einzudämmen. Zweckbindung als Prinzip kann in unterschiedlichen rechtlichen Kontexten verankert sein; es findet sich im US-amerikanischen Kontext bereits in den Fair Information Practice Principles (FIPPS) von 1973. Die USA haben allerdings weiterhin kein Datenschutzgesetz auf Bundesebene, das solche Sicherungsmechanismen verbindlich verankert.

Im europäischen Recht ist Zweckbindung ein Grundpfeiler des Datenschutzrechts und entscheidende Voraussetzung dafür, eine sekundäre Nutzung von Daten nach dem Vorgang ihrer ersten Erhebung, Ableitung oder sonstigen Erzeugung überhaupt kontrollieren zu können. Trotz expliziter Normierung in der DSGVO entfaltet der Zweckbindungsgrundsatz in der Realität nicht seine intendierte Schutzwirkung.

Der vorliegende Fall der AdTech-Industrie illustriert jedoch ein in der Literatur bereits viel diskutiertes Problem mit der Zweckbindung im Kontext von KI: KI-Modelle zur Vorhersage von Persönlichkeitseigenschaften können mit *anonymisierten* Nutzungsdaten trainiert werden und entziehen sich dann dem Schutzregime des Datenschutzes. Auch die trainierten Modelle selbst, als *abgeleitete* Datensätze, sind als anonymisierte und abgeleitete Daten regelmäßig nicht unter das Zweckbindungsgebot zu fassen. Deshalb ist der Zweckbindungsgrundsatz im Kontext von prädiktiver Analytik und KI praktisch entwertet worden: Er ist angesichts ubiquitärer Massendaten, zahlreicher beteiligter Akteure und unüberschaubarer Datenverarbeitungsvorgänge inklusive Anonymisierung nicht mehr anwendbar.

Eine Ausweitung der Zweckbindung auf KI-Modelle wäre eine Voraussetzung, um betroffenen Personen und Aufsichtsbehörden überhaupt eine Kontrolle über Datenverarbeitungsvorgänge zu ermöglichen. Denn Daten werden heute nur selten einmal erhoben und ausschließlich für einen bei der Erhebung festgelegten Zweck verarbeitet. In der Industrie ist vielmehr das Gegenteil der Fall: Daten und die aus ihnen trainierten KI-Modelle werden sekundär weiterverarbeitet und in anderen Bereichen monetarisiert. *Function creep* ist Teil des Geschäftsmodells.

Wenn nun, wie am Beispiel von ICE deutlich wird, staatliche Stellen an den KI-Modellen interessiert sind, die aus alltäglichen zivilen Datenschätzen trainiert werden, erschließt sich damit für die Industrie eine neue, vergleichsweise stabile und lukrative Einnahmequelle.

Grundlage von Datenschutz als Autonomie- und Privatheitsschutz sind zwei zentrale Elemente: zum einen die Möglichkeit, Kontrolle über die eigenen Daten auszuüben, und zum anderen der Grundsatz der „reasonable expectation of privacy“, also angemessene Erwartungen an die Privatsphäre. Beide Elemente bleiben in dieser Konstellation nicht gewahrt. Das stellt bereits im Bereich der zivilen Datenverarbeitung ein großes Problem dar, kann jedoch durch die Sekundärverwendung durch öffentliche Stellen wie ICE besonders gravierende Schäden verursachen.

Die von ICE verfolgten Personengruppen müssen um ihre körperliche Unversehrtheit und ihr Leben bangen – ebenso wie inzwischen Demonstrationsteilnehmende. Dies schlägt zugleich die Brücke zur Demokratie: um freie Diskussionen, Äußerungen, Versammlungen und letztlich Wahlen zu ermöglichen, müssen Bürger:innen in Rechtsstaaten bisher nicht damit rechnen, dass jegliche in völlig anderen Kontexten getätigte Äußerung, jahrzehntealte Facebook-Profile oder private Chats in behördlichen Verfahren herange-

zogen werden, zu denen sie keinerlei inhaltliche oder kontextuale Verbindung haben.

Zweckbindung operationalisierbar machen

Wir haben deshalb an unterschiedlichen Stellen dafür argumentiert, die Zweckbindung außerhalb des Datenschutzrechts, das stets einen identifizierbaren Datenverarbeitungsvorgang voraussetzt, zu verankern. KI-Systeme selbst, nicht individuelle Datenpunkte und ihr Personenbezug, müssen als Ansatzpunkt der Zweckbeschränkung herangezogen werden. Konkret bedeutet das: Die missbräuchliche Sekundärnutzung von Modellen der AdTech-Industrie muss verhindert werden, indem die Vorhersagemodelle selbst auf ihren zivilen Verwendungskontext festgeschrieben werden. Eine Zweckbindung allein in Bezug auf die Verarbeitung der Daten, die zur Entwicklung dieser Modelle verwendet wurden, ist demgegenüber nicht praktikabel.

Eine überprüfbare und damit vollziehbare Zweckbindung für KI-Modelle, insbesondere im Kontext von Hochrisikosystemen oder -akteuren, würde einen wichtigen Baustein eines effektiven Grundrechtsschutzes liefern. Zwecke müssen transparent kommuniziert, dokumentiert und nachvollziehbar überprüft werden. Ein erster Schritt, dies in der aktuellen EU-Digitalgesetzgebung zu verorten, wäre die Aufnahme von Zwecken und ihre Änderungen im Rahmen der KI-Datenbank nach Art. 71 KI-VO.

Darüber hinaus halten wir es für essentiell, bestimmte „Koppelungsverbote“ zu normieren. Werbe-IDs ermöglichen etwa die Erstellung umfangreicher Profile über Krankheitsprädispositionen, Sucht, sexuelle Orientierung, politische Einstellung, Konsumpräferenz und zahlreiche andere Faktoren, die in der polizeilichen Ermittlungsarbeit schon aufgrund von Diskriminierungsverboten keine Rolle spielen und zudem auch keine kriminologische Relevanz entfalten dürfen. Eine undifferenzierte Nutzung webseitenübergreifender Profile, wie z.B. durch die Meta Business Tools, sollte der Polizei nicht erlaubt sein.

Der Zweckbindungsgrundsatz sollte daher auch in der öffentlichen Beschaffung und bei der Schaffung neuer Kompetenzen stärkere Berücksichtigung finden. Staatliche Stellen sollten keine Systeme nutzen, deren Datengrundlage und vorherige Zweckbindung unklar ist oder die aus vollkommen anderen Anwendungskontexten stammen.

Datennutzung durch die deutsche Polizei

Auch in Deutschland ist der Ausbau polizeilicher Datennutzungsbefugnisse ein politisches Dauerthema. Ohne diese Diskussion in die Nähe der Vollzugspraktiken von ICE zu stellen, liegt in staatlicher Datenmacht ein Missbrauchsrisiko. Das zeigen bereits Fälle, die noch vergleichsweise analog anmuten, etwa die Abfrage von Handynummern zu privaten Zwecken. Solche Risiken potenzieren sich durch den Einsatz von KI-Technologien und durch die Zusammenarbeit mit Unternehmen wie Palantir.

Aktuelle Gesetzesänderungen in mehreren Bundesländern sehen einen erheblichen Ausbau der Datenverarbeitungsbefugnisse der Polizei vor, u.a. auch zum Training von eigenen KI-Systemen. So erlaubt etwa der neue § 24b PolG NRW eine Weiterverarbeitung von Daten zu IT-Entwicklungszwecken: Vorhandene sowie allgemein zugängliche Daten können zur Entwicklung, Überprüfung, Änderung oder zum Training von IT-Systemen verwendet werden. Darin liegt eine erhebliche Aufweichung des Zweckbindungsgrundsatzes, denn bisher war er an vergleichbare Straftaten oder den Schutz ähnlicher Rechtsgüter angeknüpft, die der ursprünglichen Erhebung zugrunde lagen.

§ 42d ASOG-G Berlin ist ähnlich angelegt, geht jedoch deutlich weiter. Die Vorschrift soll Polizei und Feuerwehr ermöglichen, Daten zum Testen und Trainieren von KI-Systemen zu verwenden, und zwar auch über die vorgesehene Speicherdauer hinaus. Absatz 3 sieht die Weitergabe von Daten an Auftragsverarbeiter und sogar an Dritte vor. Die Vorschrift höhlt damit die Zweckbindung aus, indem sie den unbestimmten Zweck „KI-Training“ ohne hinreichende rechtliche Konkretisierung legitimiert. Mangels Differenzierung nach Eingriffsintensität, Kontext oder Sensibilität der Daten sowie aufgrund des dehnbaren Vorbehalts der technischen Machbarkeit drohen zentrale Schutzmechanismen wirkungslos zu werden.

Ausblick

Der Druck auf staatliche Stellen, privatwirtschaftliche Überwachungs- und Vorhersagetechnologien zu nutzen, wird in der Zukunft eher zu- als abnehmen. Der Fall ICE zeigt, dass die Sekundärnutzung datengetriebener, ziviler Systeme – auch in rechtsstaatswidrigen Verfahrensweisen – keine hypothetische Gefahr, sondern eine ernstzunehmende Bedrohung in modernen Demokratien darstellt.

Um einerseits bei der alltäglichen Nutzung digitaler Medien die Voraussetzungen freier Meinungsbildung zu bewahren und zugleich das Potenzial für erhebliche Grundrechtseingriffe durch Missbrauch dieser mächtigen Technologien präventiv einzudämmen, sind neue und weitreichendere Schutzkonzepte erforderlich. Der gegenwärtige Stand der Datenschutzgesetzgebung und KI-Regulierung ist hierfür nicht ausreichend.

Vorsorgendes Handeln ist auch deshalb geboten, weil extensive Ausprägungen von Datenmacht nur schwer zurückgenommen werden können. Technologien, die zunächst durch vertrauenswürdig erscheinende private Akteure und für ein legitimes Ziel eingesetzt werden, können bei wechselnden politischen Mehrheiten schnell missbraucht werden. Die latente Möglichkeit, dass zivile Datentechnologie für hoheitliche Aufgaben missbraucht wird, führt zu einem gesellschaftlichen *chilling effect* auf freie Entscheidungen, Diskussionskultur, Wahlen und Grundrechtsausübung. Diese Abschreckungseffekte auf Freiheitsausübung beeinträchtigen das Gemeinwohl. So sieht es auch das Bundesverfassungsgericht: „weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen demokratischen Gemeinwesens ist."

Beide Autor:innen haben im gleichen Umfang zu diesem Artikel beigetragen.

AUTOR*INNEN

Rainer Mühlhoff
Prof. Dr. Rainer Mühlhoff, Philosoph und Mathematiker, ist Professor für Ethik der Künstlichen Intelligenz an der Universität Osnabrück. Er forscht zu Ethik, Datenschutz und kritischer Sozialtheorie in der digitalen Gesellschaft. Foto (c) 2020 Felix Noak.
Hannah Ruschemeier
Hannah Ruschemeier ist Inhaberin des Lehrstuhls für Öffentliches Recht an der Universität Osnabrück.

EMPFOHLENE ZITATION

Mühlhoff, Rainer; Ruschemeier, Hannah: Von personalisierter Werbung zur staatlichen Verfolgung: Zweckbindung als Grundrechtsschutz im Zeitalter von KI, Verfassungsblog, 03.02.2026, doi: 10.59704/8d8b05c35e77a462.

Lizensiert unter CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20260203-153209-0.