

»Ich habe nichts zu verbergen« – wirklich nicht?

Unterscheidung versus Diskriminierung durch KI, Algorithmen und die digitalen Dienste

von Indra Spiecker genannt Döhmann

Das Thema Datenschutz wird in Zeiten von Internet und künstlicher Intelligenz immer komplexer. Die Entwicklungen scheinen in manchen Bereichen kaum noch beherrschbar zu sein. Nur ein Zusammenspiel von Rechtswissenschaft und Informatik kann den Einzelnen und bestimmte gesellschaftliche Gruppen vor Diskriminierung schützen.

Über mich kann jeder alles wissen, ich habe nichts zu verbergen« – diesen Satz hört man häufig, wenn es z. B. um die Nutzung von Social Media geht oder um die Einrichtung von großen Datenbanken. Eine andere Perspektive auf den großzügigen Umgang mit den eigenen Daten tut sich vielen Gesprächspartnern dann auf, wenn man sie fragt, ob sie einem die Gehaltsbescheinigung, den Kreditkartenkontoauszug oder den Medikamentenschrank zeigen würden.

Bei genauerer Betrachtung haben die meisten Menschen eine – durchaus individuell verschiedene – Haltung dazu, was sie andere Menschen wissen lassen möchten. Und sie unterscheiden dabei sehr genau zwischen den Adressaten. Der besten Freundin und dem Sportkumpel beim Bier erzählt man andere Dinge als der Chefin oder dem Versicherungsmakler.

Mit der Kontrolle darüber, was wir wen wissen lassen, und damit einem gewissen Selbstschutz ist es aber seit geraumer Zeit vorbei, denn wir haben unsere Daten und was damit passiert oft gar nicht mehr selbst in der Hand. Seit es eine automatisierte Datenerfassung und -auswertung gibt, seit der Computer Daten sammelt, zusammenführt und beurteilt, seit also Algorithmen eingesetzt werden, können wir Menschen nicht einmal mehr sicher wissen, was mit unseren Daten geschieht – geschweige denn darauf Einfluss nehmen. Unsere Selbstschutzmechanismen greifen nicht mehr.

Datenpreisgabe an Unbekannt

Wir wissen zum einen nicht, *wer* unsere Daten hat – denn die Datenauswertung kann von den verschiedensten Unternehmen, von Privatpersonen oder vom Staat durchgeführt werden. Wer eine App auf dem Handy nutzt, gibt erhebliche Daten in aller Regel zumindest dem App-Betreiber und dem Telekommunikationsanbieter preis, der App Store hat oftmals Zugriff und zudem – bei Android-Handys – auch der Betreiber des Betriebssystems oder der Softwareplattform. Zudem gibt es eine Vielzahl von durchaus umstrittenen gesetzlichen Regelungen, die eine Herausgabe dieser Daten an staatliche Behörden ermöglichen. Und schließlich sehen die meisten App-Anbieter vor, dass die über die Nutzung der Apps gewonnenen Daten auch an Dritte weitergegeben werden können – oft ohne explizite Zustimmung der Betroffenen. Bei der Nutzung von Seiten und Angeboten im Internet ist es nicht anders: Überall werden Daten über die Nutzer erhoben und weitergegeben. In der Folge landen riesige Datenmengen über Nutzer bei den Anbietern von Digitaldiensten auf der ganzen Welt.

Wir wissen aber auch nicht, *was* über uns gewusst wird. Denn welche Daten aus welchen Quellen bei wem wie zusammengeführt werden, ist nicht überschaubar. Datenhändler tun ein Übriges, Daten über Personen, ihre Vorlieben und Abneigungen, ihr Verhalten, ihre Zahlungsbereitschaft und ihre Grenzen verfügbar zu machen.

Wie es das Bundesverfassungsgericht schon 1983 vorausschauend formuliert hat: Wer nicht weiß, was andere über ihn wissen, wird in seinem Verhalten verunsichert, weil er sich auf das Verhalten des Gegenübers nicht mehr einstellen kann. Man könnte auch sagen: Die Waffengleichheit in der Kommunikation und bei allen Entscheidungen und Verhaltensweisen wird gestört, wenn eine Seite nicht nur mehr weiß, sondern auch noch verdecken kann, was und wie viel es ist.

Wie wir beurteilt werden: Algorithmen im Einsatz

Diese Gefährdungen für den Einzelnen durch Auswertung seiner Daten unter Einsatz von automatisierter Datenverarbeitung steht seit jeher im Fokus des Datenschutzrechts; ja – dies ist sogar sein ureigenes Anliegen: das Individuum in seiner Selbstbestimmtheit und damit der Ausübung seiner Freiheitlichkeit zu schützen. Daher wohnt dem Datenschutzrecht auch durchaus nicht, wie gerne behauptet wird, per se ein paternalistisches Element inne: Es wird eben nicht – wie oft beklagt wird – die Wertung des Einzelnen, was für ihn gut ist, ersetzt durch die Wertung des Gesetzgebers, sondern das Indi-

viduum wird vielmehr in die Lage versetzt, seinen eigenen Willen zu formen und kundzutun.

Das Datenschutzrecht heute steht aber vor erweiterten Herausforderungen. Denn es geht immer weniger um die konkreten Daten eines Einzelnen, die – zusammen mit anderen Daten über diese Person – zu seinem umfassenden (Ab-)Bild zusammengesetzt werden (können). Vielmehr arbeitet moderne Datenauswertung durch Algorithmen und seit einiger Zeit auch unter Einsatz von Maschinenlernen und künstlicher Intelligenz längst damit, auf Einzeldaten möglichst weitgehend zu verzichten. Stattdessen wird der Einzelne Gruppen zugeordnet und nach den Kriterien dieser Gruppen beurteilt. Auf dieser Basis werden dann Preise für Produkte je nach Zielgruppe variabel bestimmt, werden Entscheidungen über den Zugang zu Fortbildung und Arbeitsplatz z. B. je nach sozialer Gruppenzugehörigkeit getroffen oder Krankheitsbehandlungen z. B. nach Rentabilitätskriterien zugeteilt. Wer meint, dabei handele es sich um fernliegende Szenarien autokratischer Systeme wie China oder Singapur, irrt: Für all diese Fälle gibt es Beispiele in der EU, z. T. auch in Deutschland.

Cyber-Diskriminierung als Spiegelbild unserer Gesellschaft

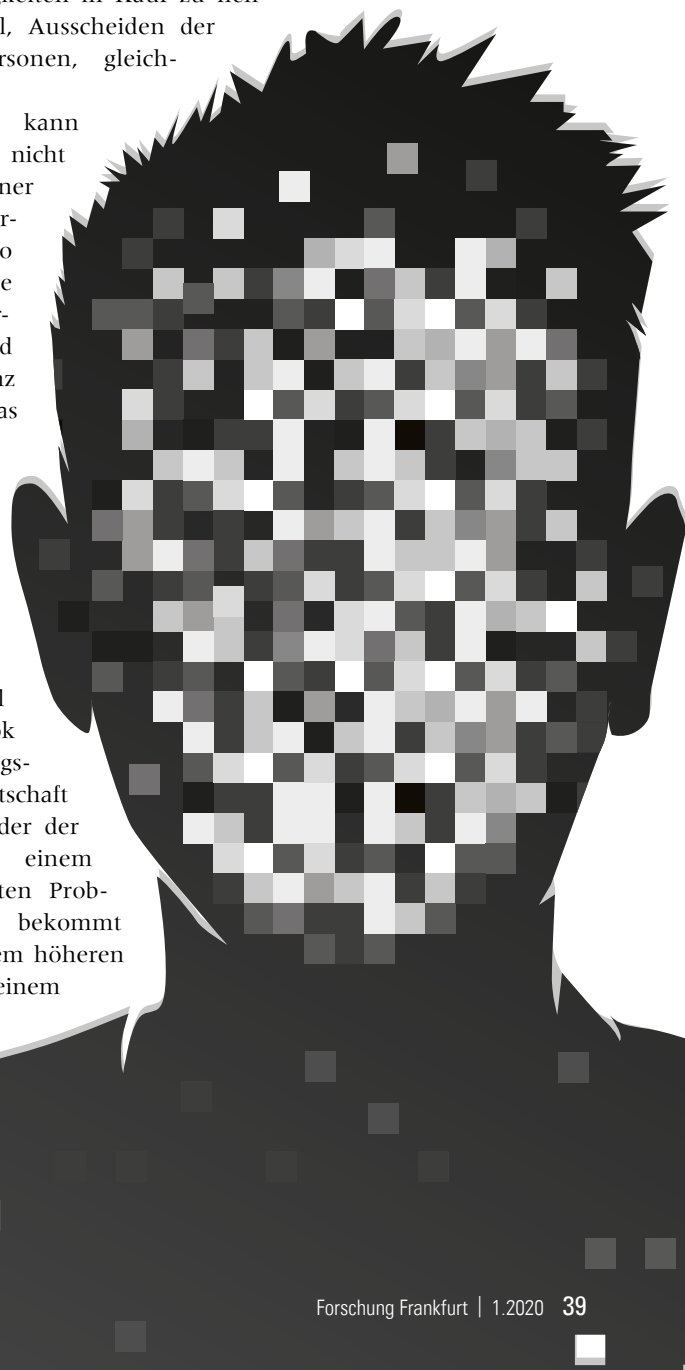
Nun wäre es vorschnell, in all diesen Fällen gleich von Diskriminierung zu sprechen. Zunächst einmal ist festzustellen: Menschen werden unterschiedlich behandelt auf der Grundlage bestimmter Vorinformationen, denen der jeweilige Entscheider in der Situation eine bestimmte Bedeutung beimisst.

Nicht jede Unterscheidung ist aber zugleich eine Diskriminierung im juristischen Sinne. Denn die Diskriminierung als rechtlicher Begriff umfasst nur die normativ unerwünschte Benachteiligung Einzelner aufgrund bestimmter Merkmale. In einigen Fällen – z. B. bei Unterscheidungen aufgrund des Geschlechts, des Glaubens oder der Rasse und Herkunft – bestimmt sogar die Verfassung in Art. 3 Abs. 3 GG, dass dies eine Diskriminierung ist. Zudem kommt es darauf an, wer unterscheidet: Der Staat unterliegt wegen des Rechtsstaatsgebots aus Art. 20 Abs. 3 GG strikteren Bindungen als Private. So dürfen Private nach Sympathie Verträge schließen, der Staat aber nicht. Inzwischen kennt aber auch das einfache Recht unterhalb der Schwelle des Verfassungsrechts Diskriminierungsverbote, z. B. im Antidiskriminierungsgesetz AGG, die insbesondere die Verweigerung eines Vertragsschlusses aufgrund bestimmter Eigenschaften untersagen – und zwar unabhängig davon, ob diese Entscheidung auf der Basis algorithmischer Auswertungen

oder individueller Entscheidungsparameter erfolgte.

Diskriminierung kann aber auch mittelbar und verdeckt erfolgen. Dazu wird ein Ersatzkriterium genutzt, das nicht auf eine Diskriminierung verweist, also neutral ist. Ist dieses Ersatzkriterium aber korreliert oder sogar eng verbunden mit dem eigentlichen Diskriminierungskriterium, ist der Erfolg derselbe: Die Benachteiligung tritt ein. Will man also z. B. geschiedene Personen nicht einstellen und weiß man (fiktiv), dass 90 Prozent aller Geschiedenen längere Zeigefinger als Mittelfinger haben, was nur bei 5 Prozent aller nicht Geschiedenen der Fall ist, kann man die diskriminierende Entscheidung aufgrund dieses neuen, scheinbar neutralen Kriteriums treffen und erreicht dasselbe Ziel. Das Beispiel zeigt zwar, dass das Ersatzkriterium möglicherweise nicht gleich aussagekräftig ist und möglicherweise auch fehlerhaft Personen aussortiert, aber wer bereit ist, diese Ungenauigkeiten in Kauf zu nehmen, wird sein Ziel, Ausscheiden der unerwünschten Personen, gleichwohl erreichen.

Und schließlich kann sich Diskriminierung nicht nur auf das Ob einer Entscheidung auswirken, sondern ebenso auf das Wie. Höhere Preise, schlechtere Vertragsbedingungen und eine geringere Kulanz können ebenso das Resultat einer Diskriminierung sein: So erhält z. B. der Nutzer eines Notebooks von Apple einen höheren Preis ausgewiesen als der Nutzer eines Discount-Notebooks, weil vom teuren Notebook auf eine hohe Zahlungsfähigkeit und -bereitschaft geschlossen wird. Oder der Hotelgast, der aus einem bundesweit bekannten Problemviertel stammt, bekommt Hotelzimmer zu einem höheren Preis als jemand aus einem



AUF DEN PUNKT GEBRACHT

- Das Gespür dafür, was man von sich selbst preisgeben möchte, ist in Zeiten der Digitalisierung außer Kraft gesetzt: Wir wissen nicht mehr, wer über welche unserer Daten verfügt und was genau damit geschieht.
- Die Auswertung großer Datenmengen führt zur Unterscheidung zwischen sozialen Gruppen. Dies muss nicht, kann jedoch im Ergebnis zu Diskriminierung führen.
- Benachteiligungen bestimmter Personengruppen sind in der digitalen Welt leichter zu kaschieren als in der realen Welt. Der Einzelne kann sich kaum dagegen wehren.
- Im Interesse des Datenschutzes müssen technische Lösungen gefunden werden, die den rechtlichen Anforderungen genügen.
- Zugleich muss das Recht so weiterentwickelt werden, dass es Antworten auf die komplexen Fragen des digitalen Zeitalters zu geben in der Lage ist.

bürgerlichen Viertel. Diese Unterscheidungen werden als personalisierte Preise oder Verträge umschrieben – ob und inwieweit sie rechtlich unerwünscht sind, ist noch heftig umstritten. Denn dass es gute und legitime Gründe für Unterscheidungen geben mag, ist offensichtlich: Wer in Vorleistung tritt, z.B. die Bank beim Kredit, der Verkäufer einer teuren Maschine oder der Vermieter einer Wohnung, möchte größtmögliche Sicherheit haben, die vereinbarte Gegenleistung auch tatsächlich zu erhalten. Eine präzise Einschätzung des Geschäftspartners z.B. hinsichtlich seines bisherigen Finanzgebarens führt dann auch zu entsprechend angepassten Bedingungen.

Der Einsatz von Algorithmen hat die bestehenden Probleme um die Diskriminierung nun erheblich verschärft. Denn war unter Bedingungen einer Offline-Welt ein Ersatzkriterium nur schwer zu finden und entsprechend leicht zu

identifizieren, sieht das bei großflächigen, statistisch ausgerichteten Datenauswertungen ganz anders aus. Nunmehr können Ersatzkriterien leicht ermittelt und eingesetzt werden, und ebenso können Preis- und Vertragsgestaltungen ohne Weiteres angepasst werden. So bekommt der Autofahrer, der häufig nachts unterwegs ist, auf der Grundlage neuartiger Telematik-Tarife schlechtere Vertragsbedingungen, weil daraus auf eine höhere Unfallwahrscheinlichkeit geschlossen wird. Für die Betroffenen ist die algorithmisch fundierte Diskriminierung eine besondere Herausforderung, denn sie ist zumeist noch weniger nachweisbar als die Diskriminierung in der Realwelt. Wie sollte der Durchschnittsnutzer herausfinden, dass über den eigenen Computer Informationen gesendet werden, aufgrund derer er schlechtere Vertragsbedingungen wie einen höheren Zimmerpreis im Hotel erhält? Wie sollte die Fernsehzuschauerin in Erfahrung bringen, dass ihre Vorliebe für eine

bestimmte Serie mit einer geringen Kreditwürdigkeit korreliert?

Und der Einsatz von Unterscheidungs-Algorithmen führt noch zu einem weiteren Problem. Damit Algorithmen ihre Rechenleistung erbringen können, müssen sie – insbesondere wenn sie im Rahmen von künstlicher Intelligenz, z.B. Maschinenlernen, eingesetzt werden – eine Vielzahl vergleichbarer Rechenoperationen durchgeführt haben, um die zugeordnete Aufgabe zuverlässig ausführen zu können. Damit aber greifen Algorithmen diejenigen Diskriminierungen auf, die sie in den vorhandenen Datensätzen vorfinden; sie können sie sogar noch verstärken. Algorithmen sind damit also beileibe weder neutral noch objektiv, sondern sie sind Abbild ihres Umfelds. Auch dies kann der Betroffene nicht kontrollieren.

Die Ohnmacht des Einzelnen

Alle diese Vorgänge sind demjenigen, der beurteilt wird, in der Regel nicht bekannt. Das überlegene Wissen über ihn selbst, das z.B. ein Datenhändler oder auch die Betreiber bekannter sozialer Medien über die Person zusammengeführt hat, steht ihm nicht zur Verfügung, und ein Recht auf Auskunft über diese aggregierten Daten besteht zumeist nicht. Auch der Entscheidung lässt sich in aller Regel nicht entnehmen, auf welcher Basis sie getroffen wurde: Ob ein Vertrag zu diesen oder jenen Bedingungen angeboten oder gänzlich verweigert wird, dass der Kindergarten- oder Studienplatz an andere vergeben wurde, lässt in aller Regel keine Rückschlüsse darauf zu, warum dies der Fall ist. Dies öffnet einerseits Tür und Tor für den Einsatz solcher Mechanismen und verschafft demjenigen, der sie verwenden kann, erhebliche Vorteile. Bei den betroffenen Personen indes werden Misstrauen und Fehleinschätzungen gesät, weil diese ihre eigenen Erklärungsansätze suchen und finden – die aber mit der realen Unterscheidung und der wirklichen Ursache gar nichts zu tun haben müssen.

Systematisch ist der Einzelne hier unterlegen, weil er die ausschlaggebende Technik der Algorithmen nicht entschlüsseln kann; und bestimmte Rechenverfahren, die gerade in der künstlichen Intelligenz wie dem Maschinenlernen oder Deep Learning eingesetzt werden, lassen es nicht einmal dann zu, wenn der Einsatz dieser Technologie bekannt ist. Wer aber nicht



nachvollziehen kann, was geschehen ist, und wer nicht das Recht und die faktische Möglichkeit hat, eine Begründung einzufordern, der kann auch nicht kritisieren, dass Rechtsverletzungen stattgefunden haben könnten.

Fazit und Ausblick

Unterscheidungen hat es immer schon gegeben; jede Entscheidung beinhaltet eine Unterscheidung, weil sie immer mindestens einer anderen Alternative eine Absage erteilt. Manchmal aber sind Unterscheidungen normativ unerwünscht, nämlich dann, wenn es sich um Diskriminierungen handelt. Diskriminierungen gilt es konsequent zu unterbinden, egal, ob sie mit oder ohne algorithmische Hilfestellung oder womöglich gar durch algorithmische Entscheidungen herbeigeführt werden. Rechtliche Vollzugs- und Durchsetzungsmechanismen stoßen hier an ihre Grenzen, denn sie basieren darauf, dass der Einzelne wehrhaft ist und seine Rechte effektiv durchsetzen kann. Gerade aber daran mangelt es. Im engen Zusammenspiel von Technologie und der Werteordnung des Rechts müssen daher technische Lösungen entwickelt werden, die den rechtlichen Anforderungen genügen. Und gleichzeitig müssen die rechtlichen Anforderungen so angepasst werden, dass sie technische Lösungen akzeptieren können. Darin liegen erhebliche Herausforderungen gleich für mehrere Forschungsansätze.

Ein erster Ansatz findet sich z. B. im Datenschutzrecht, das mit dem Konzept des »privacy by default« und »privacy by design« verlangt, dass schon die Entwicklung, erst recht aber der Einsatz von automatisierten Datenverarbeitungen rechtskonform abläuft. Ein vergleichbares Konzept könnte man auch für den Einsatz von Algorithmen fordern: Wer solche Verfahren einsetzt, muss zeigen, dass eine Diskriminierung ausgeschlossen wurde, und zwar dynamisch, d. h., es muss kontinuierlich weiterhin überprüft werden, ob eine Diskriminierung möglich geworden ist oder die Software zur Diskriminierung eingesetzt wird. Juristisch könnte man das mit Instrumenten wie Beweislastumkehr und pauschalitem Schadensersatz abfedern, so dass Verstöße sich nicht mehr lohnen würden. Je stärker nicht nur der Letztanwender in die Verantwortung genommen wird, sondern schon die unteren Ebenen bis hin zum konkreten Programmierer und dahinterstehenden Unterneh-

men, desto eher lassen sich unerwünschte Nebenwirkungen vermeiden.

Letztlich aber bedarf es eines Umdenkens seitens der Technologie, seitens der Rechtswissenschaft und seitens der Gesellschaft, und zwar schon in der Ausbildung und im Studium. IT-Entwickler brauchen ein Verständnis dafür, dass sie Sorge tragen für eine gesellschaftlich wertvolle und nicht nur finanziell ertragreiche Technologie-Entwicklung. Gesellschaftlich muss dafür eine Nachfrage gesichert sein, und dies ist nur durch eine Kenntnis und Wertschätzung für die dahinterstehenden Vorstellungen möglich. Und rechtlich müssen flankierende Normen Klarheit darüber schaffen, welche Unterscheidungen Diskriminierungen sind und wo Unterscheidung ein wettbewerbsrechtlich wichtiges Instrument für Wettbewerbsvorteile ist. Gerade der Staat ist in besonderer Weise verpflichtet, seinen eigenen Einsatz von Algorithmen aktiv kritisch zu begleiten. ●

● You can read an English translation of this article online at: www.aktuelles.uni-frankfurt.de/forschung-frankfurt-englisch



Die Autorin

Indra Spiecker genannt Döhmann, ist seit 2013 Professorin für Öffentliches Recht, Informationsrecht, Umweltrecht und Verwaltungswissenschaften und Direktorin der Forschungsstelle Datenschutz an der Goethe-Universität Frankfurt. Zuvor war sie seit 2008 am Karlsruher Institut Professorin für Technologie. Sie forscht insbesondere zu Fragen der rechtlichen Bewältigung der Digitalisierung, aber auch zu IT-Sicherheit, rechtlichen Entscheidungen unter Unsicherheit und zum Gesundheitswesen (als Direktorin des Ineges, Institut für Europäische Gesundheitspolitik und Sozialrecht). Dabei interessiert sie v. a. ein interdisziplinärer Zugang in Verbindung mit Informatik und Ökonomie. Sie ist derzeit als Sachverständige in die Kommission der Bundesregierung zur Erstellung des Dritten Gleichstellungsberichts berufen und wurde 2016 als erste Juristin in die Akademie der Technikwissenschaften acatech gewählt.

spiecker@jur.uni-frankfurt.de

