Mensch versus Maschine: Wer entscheidet was und wie?

Benedikt Buchner

Immer öfter ist von der Macht der Algorithmen zu lesen, die in allen Lebensbereichen zuzunehmen scheint. Egal, ob es um die Vermietung von Unterkünften,[1] um die Vergabe von Krediten[2] oder um Chancen am Arbeitsmarkt[3] geht – stets besteht die Befürchtung, dass der Mensch zum bloßen Objekt computergestützter Programme wird. Auch der Jubilar hat sich mit den Herausforderungen durch Algorithmen und Big Data unter den verschiedensten Aspekten auseinandergesetzt und Lösungsmöglichkeiten aufgezeigt.[4] Im Folgenden soll die Thematik aufgegriffen und im Hinblick auf automatisierte Entscheidungen erörtert werden, die in Art. 22 DS-GVO eine eigenständige Regelung erfahren haben.

Typisches Fallbeispiel für solcherlei automatisierte Entscheidungen ist die sog. algorithmendeterminierte Entscheidung, hinter der nicht mehr eine individualisierbare Einzelperson („Mensch") steht, sondern nur noch ein datengefütterter Algorithmus („Maschine"). Von diesen algorithmendeterminierten automatisierten Entscheidungen im Sinne von Art. 22 DS-GVO sind in Anlehnung an die Datenethikkommission die sog. algorithmenbasierten und algorithmengetriebenen Entscheidungen zu unterscheiden. Während sich Art. 22 DS-GVO auf ausschließlich automatisierte Entscheidungen ohne jegliches menschliche Eingreifen bezieht, agiert der Mensch bei algorithmenbasierten Entscheidungen gestützt auf algorithmisch berechnete Informationen bzw. wird bei algorithmengetriebenen

1 Zum Einsatz von Algorithmen bei Airbnb s. *Peteranderl*, So könnte Software für Airbnb Nutzer-Persönlichkeiten einschätzen, Spiegel.de v. 7.1.2020.

2 S. dazu jüngst *Hegemann*, Weiblich, Ehefrau, kreditunwürdig?, Zeit.de v. 21.11.2019.

3 Zum Algorithmus des Arbeitsmarktservice Österreich (AMS) s. *Cech/Fischer/Human/Lopez/Wagner*, Dem AMS-Algorithmus fehlt der Beipackzettel, futurezone.at v. 3.10.2019.

4 S. etwa *Skistims/Voigtmann/David/Roßnagel*, Datenschutzgerechte Gestaltung von kontextvorhersagenden Algorithmen, DuD 2012, 31; *Roßnagel/Geminn/Jandt/Richter*, Datenschutzrecht 2016 – „Smart" genug für die Zukunft?, Kassel 2016; *Löber/Roßnagel*, Kennzeichnung von Social Bots, MMR 2019, 493.

https://doi.org/10.5771/9783748910770-289

Entscheidungen in seinem Entscheidungsspielraum durch die algorithmisch berechneten Informationen beschränkt.[5]

I. Automatisierte Entscheidungen: drei Schutzperspektiven

Automatisierte Entscheidungen können aus dreierlei Perspektiven betrachtet werden: aus der Perspektive des Datenschutzes, aus der des Diskriminierungsschutzes und, last but not least, aus der Perspektive eines „Schutzes vor der Maschine".

Datenschutz betrifft zunächst die Frage der Datengrundlage, auf deren Basis dann Entscheidungen getroffen werden. Soweit es um Entscheidungen auf der Grundlage von personenbezogenen Daten geht, handelt es sich um eine datenschutzrechtliche Frage. Zentral ist hier, ob und unter welchen Voraussetzungen Algorithmen überhaupt mit personenbezogenen Daten gespeist werden dürfen, auf deren Grundlage dann diese oder jene Entscheidung zugunsten oder zulasten einer bestimmten Person getroffen wird.

Eine andere rechtliche Herausforderung ist die des Diskriminierungsschutzes. Eine besondere Problematik algorithmendeterminierter Entscheidungen ist gerade darin zu sehen, dass diese zu Entscheidungen führen können, die Personen mit bestimmten Eigenschaften in besonderem Maße benachteiligen. Um insoweit Diskriminierungen zu vermeiden, kann an zwei Stellen angesetzt werden: Zum einen kommt ein unmittelbarer Diskriminierungsschutz in Form von Diskriminierungsverboten in Betracht.[6] Zum anderen kann eine Diskriminierung aber möglicherweise schon dadurch unterbunden werden, dass von vornherein überhaupt keine Kenntnis von diskriminierungsrelevanten Daten erlangt wird. Insoweit kommt dann also wieder der Datenschutz ins Spiel.

Drittens schließlich muss das Recht Vorgaben machen, ob und inwieweit Maschinen überhaupt dazu legitimiert sein sollen, über Menschen zu entscheiden. Die Risiken und Chancen algorithmendeterminierter Entscheidungen sind adäquat zu berücksichtigen. Weder menschliche noch automatisierte Entscheidungsfindungen sind per se besser oder schlechter. Ohnehin können Mensch und Maschine (sowie deren Entscheidungen) nicht isoliert voneinander betrachtet werden, da hinter maschinengesteu-

5 *DEK*, Gutachten der Datenethikkommission, 2019, 24.

6 Zu einer möglichen Fortschreibung des Antidiskriminierungsrechts s. *DEK* (Fn. 5), 193 f.

https://doi.org/10.5771/9783748910770-289

erten Entscheidungsprozessen regelmäßig von Menschen programmierte Grundannahmen und Zielvorgaben stehen.[7] Im geltenden Recht adressiert diesen Aspekt bislang in erster Linie Art. 22 DS-GVO, der – obwohl in einem datenschutzrechtlichen Regelwerk verankert – dem Grunde nach keine spezifisch datenschutzrechtliche Regelung darstellt, sondern vielmehr die Grundsatzfrage betrifft, ob und inwieweit Maschinen überhaupt Entscheidungen treffen dürfen.

II. Datenschutz

Das Datenschutzrecht begrenzt in vielerlei Hinsicht schon im Vorfeld die Möglichkeiten für eine automatisierte Entscheidung, indem es an der Datengrundlage einer solchen Entscheidung ansetzt. Im Vorfeld einer automatisierten Entscheidung steht zunächst die vorbereitende automatisierte Verarbeitung personenbezogener Daten, die von der eigentlichen Entscheidung zu trennen ist.[8] Je weniger „frei" Maschinen in der Verarbeitung personenbezogener Daten sind, desto begrenzter ist von vornherein ihr Entscheidungsspielraum. Konkrete (datenschutzrechtliche) Grenzen für die vorgeschaltete Datenverarbeitung durch Maschinen fußen dabei in erster Linie auf dem datenschutzrechtlichen Verbotsprinzip, dem Grundsatz der Zweckbindung, den Grundsätzen der Datenminimierung, Speicherbegrenzung und Richtigkeit der Datenverarbeitung sowie dem Transparenzprinzip.[9]

1. Verbotsprinzip

Kernidee eines Algorithmus ist es, ein bestimmtes Problem durch eine endliche Sequenz von Berechnungsschritten zu lösen.[10] Im Zeitalter von Big Data ist je nach Art des Algorithmus gerade die Eingabe möglichst vie-

---

7 Ausführlich *Martini*, Blackbox Algorithmus, Berlin 2019, 47 ff.

8 *Schulz*, in: Gola (Hrsg.), DS-GVO, 2. Aufl., München 2018, Art. 22 DS-GVO, Rn. 12; *Scholz*, in: Simitis/Hornung/Spiecker (Hrsg.), Datenschutzrecht, Baden-Baden 2019, Art. 22 DS-GVO, Rn. 17.

9 *Buchner*, Big Data und Datenschutz im Gesundheitswesen, ZfmE 2018, 131, 135 ff.

10 Ausführlicher dazu *Aho/Hopcroft/Ullmann*, Data Structures and Algorithms, Reading 1987, 2.

https://doi.org/10.5771/9783748910770-289

ler Daten erforderlich oder sogar erwünscht und vor allem im Bereich des Machine Learning werden Unmengen an Daten verarbeitet.

Das Datenschutzrecht deutscher und europäischer Prägung steht einem solchen Phänomen der exzessiven Datenverarbeitung zunächst einmal diametral entgegen, weil es im Ausgangspunkt ein pauschales Verbot der Verarbeitung personenbezogener Daten vorsieht. Jede Form der Datenverarbeitung ist nach Art. 6 Abs. 1 DS-GVO unzulässig – es sei denn, die von der Datenverarbeitung betroffene Person hat in diese wirksam eingewilligt (Art. 6 Abs. 1 lit. a DS-GVO) oder die Datenverarbeitung lässt sich auf einen der sonstigen in Art. 6 Abs. 1 DS-GVO normierten Erlaubnistatbestände (lit. b bis f) stützen. Für die Verarbeitung besonders sensibler Daten i.S.d. Art. 9 DS-GVO ist das Verbotsprinzip noch einmal ausdrücklich in Art. 9 Abs. 1 DS-GVO normiert.

Das Verbotsprinzip ist eine klare Grundsatzentscheidung für einen effektiven Schutz informationeller Selbstbestimmung und gegen eine grenzenlose Datenverarbeitung.[11] Nichtsdestotrotz ist das Datenschutzrecht aber auch in dieser strengen Prägung keine unüberwindbare Hürde für eine Datenverarbeitung – auch nicht für eine Datenverarbeitung im Dienste von Algorithmen und Big Data.[12] Selbstverständlich stellt auch die DS-GVO in Rechnung, dass die Ziele und Interessen, die mit einer Verarbeitung personenbezogener Daten verfolgt werden, so gewichtig sein können, dass sie die Schutzbedürftigkeit personenbezogener Daten überwiegen. Und eben deshalb sieht das Datenschutzrecht zahlreiche Erlaubnistatbestände für eine Datenverarbeitung vor – allen voran den Erlaubnistatbestand des Art. 6 Abs. 1 lit. f DS-GVO, dessen Interessenabwägung je nach Auslegung einen sehr weiten Spielraum für eine Datenverarbeitung eröffnen kann. Damit ist eine Datenverarbeitung in weitem Umfang auch unter dem vermeintlich so strengen Verbotsprinzip möglich, allerdings verbunden mit einer Art von Rechtfertigungslast für die datenverarbeitende Stelle: Big Data muss sich als „Verantwortlicher" dafür rechtfertigen, möglichst viele Daten verarbeiten zu wollen – und eben nicht der Einzelne dafür, dass er „seine" personenbezogenen Daten nicht verarbeitet sehen möchte.

11 Kritisch zum Begriff des Verbotsprinzips s. *Roßnagel*, Kein „Verbotsprinzip" und kein „Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht, NJW 2019, 1.

12 *Buchner*, ZfmE 2018 (Fn. 9), 135.

https://doi.org/10.5771/9783748910770-289

2. Zweckbindung

Nach Art. 5 Abs. 1 lit. b DS-GVO müssen personenbezogene Daten „für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden". Daten dürfen also gerade nicht auf Vorrat gesammelt werden, um sie dann mittels Big Data-Anwendungen beliebig als Datenbasis für automatisierte Entscheidungen zu nutzen.[13] Vom Regelungskonzept ist auch hier wieder zwischen der automatisierten Entscheidung einerseits und der dieser Entscheidung zugrundeliegenden Datenverarbeitung andererseits zu differenzieren.[14] Für den der Entscheidung zugrundeliegenden Datenverarbeitungsprozess bedeutet dann der Zweckbindungsgrundsatz: Die Datenverarbeitung als Grundlage für eine automatisierte Entscheidung ist nur dann zulässig, wenn personenbezogene Daten von vornherein gerade für diesen Zweck erhoben worden sind oder aber wenn im Fall einer Weiterverarbeitung zu diesem (anderen als dem ursprünglichen) Zweck diese wieder auf einen Erlaubnistatbestand gestützt werden kann *und* der Zweck der Weiterverarbeitung sich mit dem ursprünglichen Erhebungszweck vereinbaren lässt.[15]

Für letztere Frage der Vereinbarkeit normiert Art. 6 Abs. 4 DS-GVO eine Reihe von Beurteilungskriterien, die gerade für die Datenverarbeitung im Dienste von Algorithmen und Big Data oftmals nur schwer zu erfüllen sein werden. Das gilt schon für das Kriterium der „Verbindung" zwischen dem ursprünglichen Zweck der Datenerhebung und dem neuen Zweck der Datenverarbeitung (lit. a): Je weiter der Zweck der ursprünglichen Verarbeitung und der Zweck der Weiterverarbeitung auseinanderliegen, desto mehr spricht dies gegen eine Vereinbarkeit der beiden Zwecksetzungen. Big Data und dessen Nutzung für automatisierte Entscheidungen zeichnen sich aber gerade auch dadurch aus, dass überraschende und so nicht erwartete Korrelationen ausfindig gemacht und Entscheidungen zugrunde gelegt werden. Des Weiteren werden insbesondere auch die „möglichen Fol-

---

13 Zum Zweckbindungsgrundsatz s. schon BVerfGE 65, 1 (46): „Damit wäre die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren."

14 S. schon oben Fn. 8.

15 Art. 6 Abs. 4 DS-GVO selbst ist kein Erlaubnistatbestand für eine zweckändernde Datenverarbeitung; s. *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl., München 2020 i.E., Art. 6 DS-GVO, Rn. 181 ff.; a.A. *Richter*, Big Data, Statistik und die DS-GVO, DuD 2016, 581, 584 und auch *Roßnagel*, in: Simitis/Hornung/Spiecker (Hrsg.) (Fn. 8), Art. 6 Abs. 4, Rn. 12.

https://doi.org/10.5771/9783748910770-289

gen“ der beabsichtigten Weiterverarbeitung für den Betroffenen (lit. d) oftmals gegen eine Vereinbarkeit sprechen, vor allem dann, wenn die Datenverarbeitung darauf abzielt, einzelne Personen in einer bestimmten Art und Weise zu kategorisieren und daran möglicherweise auch negative Konsequenzen zu knüpfen. In diesem Zusammenhang ist überdies auch zu berücksichtigen, dass es für die betroffene Person im Kontext von Big Data und Algorithmen regelmäßig besonders schwer ist, die Weiterverarbeitung ihrer Daten im Einzelnen nachvollziehen und ihre Folgen abschätzen zu können.[16]

Im Ergebnis begrenzt damit der Zweckbindungsgrundsatz die Datengrundlage, auf die sich automatisierte Entscheidungen stützen können, erheblich. Zwar sind in der DS-GVO Ausnahmen vom Zweckbindungsgrundsatz durchaus vorgesehen, aber eben nur für bestimmte, aus Sicht des Gesetzgebers besonders privilegierungswürdige Zwecke der Datenverarbeitung. Eine solche Ausnahme ist beispielsweise für die Datenverarbeitung zu wissenschaftlichen Forschungszwecken normiert. Art. 5 Abs. 1 lit. b DS-GVO sieht hier eine Privilegierung der Datenverarbeitung vor, indem eine Vereinbarkeit mit den ursprünglichen Verarbeitungszwecken fingiert wird, wenn die Daten für wissenschaftliche Forschungszwecke weiterverarbeitet werden. Allerdings reicht allein der Umstand, dass Big Data-Anwendungen stets auch auf eine wie auch immer im Einzelnen ausgestaltete „wissenschaftliche Vorgehensweise“ verweisen können, nicht aus.[17] So spricht die DS-GVO bewusst von wissenschaftlichen Forschungszwecken in Abgrenzung zum allgemeineren Begriff der „wissenschaftlichen Zwecke“, um sicherzustellen, dass nicht jede Analyse und Aufbereitung von Daten eine Privilegierung als Wissenschaft beansprucht.[18] Entscheidend für eine Privilegierung als Wissenschaft ist das Ziel einer transparenten Wissensgenerierung für die Allgemeinheit. Davon zu unterscheiden sind kommerziell motivierte Datenverarbeitungsprozesse im Forschungsgewand, mit denen Datenverarbeiter in erster Linie auf eine Verbesserung der eigenen Bilanz und Wettbewerbsposition abzielen.[19]

---

16 *Martini*, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017, 1018; in diesem Sinne für Big Data in der Medizin schon *Buchner*, ZfmE 2018 (Fn. 9), 135.

17 *Richter*, Datenschutz zwecklos? – Das Prinzip der Zweckbindung im Ratsentwurf der DS-GVO, DuD 2015, 735, 737 f.; *Roßnagel/Nebel/Richter*, Was bleibt vom Europäischen Datenschutzrecht?, ZD 2015, 455, 457 f.

18 *Albrecht*, in: Albrecht/Jotzo (Hrsg.), Das neue Datenschutzrecht der EU, Baden-Baden 2017, Teil 3, Rn. 71.

19 *Buchner/Tinnefeld*, in: Kühling/Buchner (Hrsg.) (Fn. 15) Art. 89 DS-GVO, Rn. 13.

https://doi.org/10.5771/9783748910770-289

3. Datenminimierung, Speicherbegrenzung und Richtigkeit

Auch die datenschutzrechtlichen Grundsätze der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO), der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DS-GVO) und der Richtigkeit (Art. 5 Abs. 1 lit. d DS-GVO) sind regelmäßig nur schwer vereinbar mit den Zielen von Big Data und Co. Das, worauf automatisierte Entscheidungen im Kontext von Big Data angewiesen sind, nämlich die Verarbeitung von möglichst vielen Daten für unbestimmte Zeit, soll durch die Grundsätze der Datenminimierung und Speicherbegrenzung gerade begrenzt werden. Und auch unter dem Aspekt der Richtigkeit ist die Legitimation automatisierter Entscheidungen oftmals fragwürdig. Je mehr Daten verarbeitet werden, desto höher ist auch das Risiko, dass unrichtige Daten verarbeitet werden, vor allem wenn den betroffenen Personen Daten falsch zugeordnet werden. Problematisch ist diese Fehleranfälligkeit vor allem auch mit Blick auf die Intransparenz der Datenverarbeitung. Für den Einzelnen ist eine Kontrolle der Richtigkeit der Datenverarbeitung beim Einsatz von Algorithmen regelmäßig unmöglich. Konfrontiert wird dieser allein mit dem Ergebnis von Rechenprozessen: der Bewertung in Form eines bestimmten Scores oder der Einordnung in eine bestimmte Kategorie als „vertrauenswürdig", „riskant" oder Ähnliches. Die Algorithmen, auf denen derlei Einordnungen beruhen, sind für den einzelnen Betroffenen regelmäßig undurchschaubar und werden als „Geschäftsgeheimnis" streng gehütet – mit der Konsequenz, dass eine Kontrolle, ob die in den Algorithmus eingespeisten Daten „sachlich richtig" und „auf dem neuesten Stand" i. S. d. Art. 5 Abs. 1 lit. d DS-GVO sind, überhaupt nicht möglich ist.

4. Transparenzproblem

Die Antworten des Datenschutzrechts auf die gerade angesprochenen Probleme sind bislang wenig befriedigend: Zwar wird Transparenz immer wieder betont – so auch im Gesetzgebungsverfahren zur DS-GVO – und spielt auf dem Papier eine zentrale Rolle. Sichtbarster Ausdruck sind die umfangreichen Informationspflichten nach den Art. 13 und 14 DS-GVO. Regelmäßig bleibt jedoch die tatsächliche Umsetzung hinter all den rechtlichen Vorgaben zurück.[20] Mehr noch: Oftmals verkehrt sich Transparenz

20 Für den Bereich der Online-Dienste s. *Helmschrot/Wiebe*, Untersuchung der Umsetzung der DS-GVO durch Online-Dienste, 2019.

https://doi.org/10.5771/9783748910770-289

sogar in ihr Gegenteil und führt im Ergebnis zu einer Informationsüberflutung bei den betroffenen Personen infolge überlanger Phrasentexte. Was die an sich relevanten Stellschrauben einer Datenverarbeitung anbelangt, herrscht viel zu oft Unkenntnis auf Seiten der Betroffenen, gerade auch wenn es um die Datenbasis automatisierter Entscheidungen geht.

Ein Streitpunkt von zentraler Bedeutung ist in diesem Zusammenhang die Frage, ob die Informations- und Auskunftspflichten aus Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g sowie Art. 15 Abs. 1 lit. h DS-GVO, wenn sie sich auf die „involvierte Logik" einer automatisierten Entscheidung beziehen, dahingehend zu verstehen sind, dass sie auch zur Offenlegung der einer Entscheidung zugrunde liegenden Scoreformeln und Algorithmen verpflichten.[21] Der BGH hat, allerdings noch unter dem alten Recht, im Fall der SCHUFA eine Verpflichtung zur Offenlegung der SCHUFA-Scoreformel abgelehnt; ausschlaggebend war für den BGH in erster Linie der Schutz von Geschäftsgeheimnissen.[22] Der Gerichtshof zählte zu den als Geschäftsgeheimnis geschützten Inhalten sowohl die in die Scoreformel einfließenden allgemeinen Rechengrößen, wie etwa die herangezogenen statistischen Werte, als auch die Gewichtung einzelner Berechnungselemente bei der Ermittlung des Wahrscheinlichkeitswerts sowie die Bildung etwaiger Vergleichsgruppen als Grundlage der sog. Scorekarten.

Unter Geltung der DS-GVO lässt sich diese Einschränkung der Informationspflichten durch den BGH nicht mehr aufrechterhalten[23] – schon mit Blick auf das Kernanliegen des europäischen Gesetzgebers, mit der Reform des Datenschutzrechts vor allem auch die Transparenz der Datenverarbeitung zu fördern und die von der Datenverarbeitung betroffene Person dahingehend zu stärken, ihre Rechte möglichst effektiv auszuüben.[24] Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g und Art. 15 Abs. 1 lit. h DS-GVO fordern ausdrücklich „aussagekräftige Informationen" über die involvierte Logik. Die Einschränkungen des BGH bleiben hinter dieser Anforderung weit zurück.[25] Informationen, die sich allein auf die Datengrundlage eines Sco-

21 Für eine Pflicht zur Information über den verwendeten Algorithmus u.a. *Roßnagel/Nebel/Richter,* ZD 2015 (Fn. 17), 458.

22 BGH, Urt. v. 28.1.2014 – VI ZR 156/13, Rn. 27 zum Auskunftsrecht nach § 34 Abs. 4 S. 1 Nr. 4 BDSG aF.

23 Vgl. hierzu und zum Folgenden *Buchner*, in: Kühling/Buchner (Hrsg.) (Fn. 15) Art. 22 DS-GVO, Rn. 35 f.

24 *Albrecht*, in: Albrecht/Jotzo (Hrsg.), Das neue Datenschutzrecht der EU, Baden-Baden 2017, Teil 1, Rn. 8 und Teil 2, Rn. 3 f.; *Dix*, in: Simitis/Hornung/Spiecker (Hrsg.) (Fn. 8), Art. 15 DS-GVO, Rn. 25.

25 Vgl. auch *Schmidt-Wudy,* in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, 30. Ed., München 2019, Art. 15 DS-GVO, Rn. 78.3.

https://doi.org/10.5771/9783748910770-289

ring (oder sonstigen Profiling) beschränken, können kaum einen „aussagekräftigen" Eindruck davon vermitteln, welche Logik involviert ist, wenn über den Betroffenen mittels Punkten o.Ä. ein Urteil gefällt wird. Damit die betroffene Person die ihr zugeschriebenen Scorewerte u.Ä. zumindest in Grundzügen nachvollziehen kann, müssen ihr Informationen zur Gewichtung der in die Beurteilung eingeflossenen Faktoren, zur einschlägigen Vergleichsgruppe sowie zu den Gründen, weshalb sie dieser Vergleichsgruppe zugeordnet wurde, erteilt werden, um die informationellen Asymmetrien zwischen Betroffenen und Datenverarbeitern zumindest teilweise abzufedern.[26]

III. Diskriminierungsschutz

Die Komplexität und Undurchschaubarkeit automatisierter Entscheidungen ist nicht nur ein Datenschutz-, sondern auch ein Diskriminierungsproblem. Je mehr Daten gesammelt werden und je häufiger Algorithmen zum Einsatz kommen, um Personen nach bestimmten Eigenschaften zu kategorisieren und dementsprechend Entscheidungen zu treffen, desto deutlicher treten Ungleichheiten zutage und desto größer ist das damit einhergehende Diskriminierungspotenzial.

1. Besondere Risiken

Automatisierte Entscheidungen über Personen auf der Basis intransparenter Algorithmen sind vor allem deshalb problematisch, weil damit stets auch die Gefahr einhergeht, dass solcherlei Entscheidungen auf Eigenschaften gestützt werden, die ein besonderes Diskriminierungspotenzial bergen. Exemplarisch ist der Einsatz von COMPAS („Correctional Offender Management Profiling for Alternative Sanctions") in den USA – eine Software, die algorithmenbasiert die Wahrscheinlichkeit für die Rückfälligkeit oder auch Gefährlichkeit von Straftätern berechnen und auf diese Weise Richterinnen und Richter bei ihren Entscheidungen unterstützen sollte. Letztlich hat sich herausgestellt, dass diese vermeintlich objektiven datenbasierten „Berechnungen" mindestens ebenso diskriminierungs- und

26 *Buchner*, in: Kühling/Buchner (Hrsg.) (Fn. 15), Art. 12 DS-GVO, Rn. 35a; *Dix*, in: Simitis/Hornung/Spiecker (Hrsg.) (Fn. 8), Art. 15 DS-GVO, Rn. 25.

https://doi.org/10.5771/9783748910770-289

fehleranfällig wie menschliche Entscheidungen waren.[27] Demselben Vorwurf sieht sich eine Software ausgesetzt, die – ebenfalls in den USA – von Krankenhäusern und Versicherungen eingesetzt worden ist, um diejenigen Patienten zu identifizieren, die vorzugsweise eine aufwändigere und kostenintensivere Behandlung erhalten sollen. Im Ergebnis hat der Einsatz dieser Software infolge missglückter Korrelationen dazu geführt, dass in erster Linie für Afroamerikaner der Zugang zu einer intensiveren medizinischen Betreuung erschwert wurde.[28]

2. *Datenschutz als präventiver Diskriminierungsschutz*

Einen Schutz vor diskriminierenden Konsequenzen kann – mittelbar – auch das Datenschutzrecht gewährleisten, indem dieses vorgeschaltet mittels Verboten sicherstellt, dass Informationen, die ein besonderes Diskriminierungspotenzial bergen, erst gar nicht zur Kenntnis genommen und damit auch nicht als Grundlage für automatisierte Entscheidungen herangezogen werden können. Möglichen Diskriminierungen wird schlichtweg von vornherein die erforderliche Informationsgrundlage vorenthalten.[29] Zentrale Scharniernorm ist insoweit Art. 9 DS-GVO, der die Zulässigkeit einer Verarbeitung von sog. besonderen Kategorien personenbezogener Daten regelt, die vom Gesetzgeber als besonders schutzwürdig angesehen werden. Art. 9 Abs. 1 DS-GVO zählt zu diesen besonders schutzwürdigen Daten gerade diejenigen Merkmale, die auch als besonders diskriminierungsanfällig einzustufen sind und die sich daher so auch in Art. 21 GRCh (Nichtdiskriminierung) wiederfinden.[30] Indem eine Verarbeitung dieser besonders schutzwürdigen Daten nach Art. 9 Abs. 1 DS-GVO grundsätzlich untersagt wird, fungiert dieses Verbotsprinzip insoweit also auch als „informationelles Diskriminierungsverbot“[31]; Datenschutz wird so zu einer Art von „präventivem Diskriminierungsschutz“.[32]

---

27 *Bertelsmann Stiftung*, Wenn Maschinen Menschen bewerten. Internationale Fallbeispiele für Prozesse algorithmischer Entscheidungsfindung - Arbeitspapier -, Bertelsmann Stiftung (Hrsg.), 2017, 9 f.

28 *Beuth/Breithut*, Diskriminierender Algorithmus – Patienten-Algorithmus benachteiligt Millionen Afroamerikaner, Spiegel.de v. 25.10.2019.

29 *Buchner*, ZfmE 2018 (Fn. 9), 138.

30 *Weichert*, Sensitive Daten revisited, DuD 2017, 538, 539.

31 *Weichert*, in: Kühling/Buchner (Hrsg.) (Fn. 15), Art. 9 DS-GVO, Rn. 2.

32 *Rieble*, Anm. zu BAG (11.11.1993), EzA Nr. 40 zu § 123 BGB, 13.

https://doi.org/10.5771/9783748910770-289

3. Ungleichbehandlung und/oder Diskriminierung?

So konfliktträchtig automatisierte Entscheidungen hinsichtlich ihres Diskriminierungspotenzials sind: Nicht jede Ungleichbehandlung, auch wenn sie auf automatisierten Entscheidungen beruht, stellt zugleich eine unzulässige Diskriminierung im rechtlichen Sinne dar.[33] Auch das Allgemeine Gleichbehandlungsgesetz (AGG) zielt nicht darauf ab, für eine ausnahmslose Gleichbehandlung aller zu sorgen, sondern darauf, Unterscheidungsmerkmale zu unterbinden, denen ein besonderes Diskriminierungspotenzial innewohnt: Rasse und ethnische Herkunft, Geschlecht, Religion und Weltanschauung, Behinderung, Alter oder sexuelle Identität. Und selbst im Fall dieser besonders diskriminierungsanfälligen Merkmale geht es im Antidiskriminierungsrecht nicht darum, durchgängig sämtliche Ungleichheiten zu nivellieren. So regelt § 20 Abs. 1 S. 1 AGG für den Diskriminierungsschutz im Zivilrechtsverkehr ausdrücklich, dass eine Verletzung des Benachteiligungsverbots nicht anzunehmen ist, wenn „für eine unterschiedliche Behandlung wegen der Religion, einer Behinderung, des Alters, der sexuellen Identität oder des Geschlechts ein sachlicher Grund vorliegt". „Diskriminierend" (oder ungerechtfertigt diskriminierend[34]) ist also nicht automatisch jede unterschiedliche Behandlung, die mit einer Benachteiligung einhergeht, sondern nur die „rechtswidrige, sozial verwerfliche Ungleichbehandlung".[35]

Für den Versicherungsbereich konkretisiert § 20 Abs. 2 S. 2 AGG den sachlichen Grund dahingehend, dass eine unterschiedliche Behandlung zulässig ist, wenn sie „auf anerkannten Prinzipien risikoadäquater Kalkulation beruht, insbesondere auf einer versicherungsmathematisch ermittelten Risikobewertung unter Heranziehung statistischer Erhebungen". Derselbe Ansatzpunkt findet sich auch im Datenschutzrecht, wenn für die Zulässigkeit einer Risikobewertung in Gestalt des Scoring darauf abgestellt wird, ob die zur Score-Berechnung genutzten Daten „unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind". Der Sache nach ist also beim Datenschutz wie beim Diskriminierungsschutz die – nachvollziehbare – Rationa-

---

33 Vgl. dazu auch *Buchner*, Informationelle Selbstbestimmung im Privatrecht, Tübingen 2006, 195 f.

34 Zur dogmatischen Einordnung des § 20 AGG als Rechtfertigungsgrund *Thüsing*, in: Säcker/Rixecker/Oetker/Limperg (Hrsg.), Münchener Kommentar zum BGB, 8. Aufl., München 2018, § 20 AGG, Rn. 3.

35 Begründung zum Regierungsentwurf des AGG, BT-Drs. 16/1780, 30.

https://doi.org/10.5771/9783748910770-289

lität des Entscheidungsprozesses ein ganz zentraler Faktor. Unter Datenschutz- wie unter Diskriminierungsschutzgesichtspunkten gilt für automatisierte Entscheidungsprozesse, dass diese nicht auf einer unzureichenden Datenbasis, auf einem fehlerhaften statistischen Verfahren oder auf irgendwelchen nicht rationalisierbaren Intuitionen des Verantwortlichen beruhen dürfen.[36] Ebenso sind auch automatisierte Entscheidungen auf Grundlage selbstlernender Algorithmen, da nicht hinreichend dokumentierbar und damit auch nicht nachvollziehbar, grundsätzlich unzulässig.[37]

IV. Schutz „vor der Maschine" (Art. 22 DS-GVO)

Auch die Grundsatzfrage, ob Maschinen und Algorithmen überhaupt über Menschen entscheiden sollen und dürfen, wird vom Recht adressiert – so bereits unter der Datenschutz-Richtlinie mit Art. 15 DSRL und nunmehr unter der DS-GVO mit Art. 22. Dabei wird die Frage im Ausgangspunkt zunächst einmal mit einem dezidierten „Nein" beantwortet. Kernanliegen des Art. 22 DS-GVO (ebenso wie schon des Art. 15 DSRL) ist es, den Einzelnen davor zu schützen, dass Entscheidungen über ihn allein auf Grundlage einer automatisierten Bewertung seiner Persönlichkeitsmerkmale gefällt werden und er so zu einem bloßen Objekt computergestützter Programme wird.[38] Entsprechend räumt die Vorschrift der betroffenen Person das Recht ein, „nicht einer ausschließlich auf einer automatisierten Verarbeitung […] beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt."

Art. 22 DS-GVO ist keine Vorschrift im klassischen datenschutzrechtlichen Sinne, sie regelt allein die Zulässigkeit der automatisierten Entscheidung selbst, nicht aber die Zulässigkeit der Datenverarbeitung, die dieser Entscheidung vorgeschaltet ist. Für diese Datenverarbeitung gelten vielmehr die allgemeinen Regeln der DS-GVO.[39] Art. 22 DS-GVO ergänzt die-

---

36 S. (allerdings kritisch) zu dieser „Basisrationalität" *Gerberding/Wagner*, Qualitätssicherung für "Predictive Analytics" durch digitale Algorithmen, ZRP 2019, 116, 118; s.a. *Weichert*, in: Däubler/Wedde/Weichert/Sommer (Hrsg.), EU-DS-GVO und BDSG-neu, Frankfurt am Main 2018, § 31 BDSG, Rn. 13.

37 *Weichert*, in: Däubler/Wedde/Weichert/Sommer (Hrsg.) (Fn. 36), § 31 BDSG, Rn. 13.

38 *Buchner*, in: Kühling/Buchner (Hrsg.) (Fn. 15), Art. 22 DS-GVO, Rn. 1; *Scholz*, in: Simitis/Hornung/Spiecker (Hrsg.) (Fn. 8), Art. 22 DS-GVO, Rn. 3.

39 *Schulz*, in: Gola (Hrsg.) (Fn. 8), Art. 22 DS-GVO, Rn. 3.

https://doi.org/10.5771/9783748910770-289

se allgemeinen datenschutzrechtlichen Vorgaben, die Rede ist insoweit auch von einer „flankierende[n] Verfahrensvorschrift zu den eigentlichen datenschutzrechtlichen Erlaubnistatbeständen".[40] Der Einzelne soll, wie gerade schon angesprochen, nicht zu einem „bloßen Objekt von Computeroperationen degradiert" werden, die Verantwortung für Entscheidungen über Menschen soll nicht allein anonymen Computersystemen überantwortet werden.[41]

Der Schutz „vor der Maschine" durch Art. 22 DS-GVO ist allerdings kein absoluter. Als schutzbedürftig wird der Einzelne nur dann eingeordnet, wenn es um ausschließlich automatisierte Entscheidungen ohne jegliches menschliche Eingreifen geht, nach der Terminologie der Datenethikkommission also um sog. algorithmendeterminierte Entscheidungen, hinter denen überhaupt keine individualisierbare Einzelperson mehr steht, sondern ausschließlich ein datengefütterter Algorithmus. Im Unterschied dazu ist bei sog. algorithmenbasierten Entscheidungen nicht die Maschine, sondern immer noch ein Mensch verantwortlich, weil dieser seine Entscheidung lediglich auf algorithmisch berechnete (Teil-)Informationen stützt. Auch die sog. algorithmengetriebenen Entscheidungen sind nach dem Verständnis der Datenethikkommission noch „menschliche Entscheidungen", auch wenn diese dadurch geprägt sind, dass die Ergebnisse algorithmischer Systeme den tatsächlichen Entscheidungsspielraum einschränken.[42] Zu Recht weist die Datenethikkommission aber auch darauf hin, dass sich in der Praxis der Einfluss solcher algorithmenbasierter oder -getriebener Entscheidungssysteme nahezu ebenso stark auswirken kann wie der von algorithmendeterminierten Systemen und es daher langfristig auch insoweit eines Regulierungsregimes bedarf.[43] Die Datenethikkommission empfiehlt hierfür einen risikoadaptierten Regelungsansatz: Algorithmische Systeme sollen abhängig vom drohenden Schaden für Verbraucherrechte in fünf Risikoklassen eingeteilt werden und Algorithmen mit „unvertretbarem Schädigungspotenzial" sollen verboten werden können.[44]

---

40 *Von Lewinski*, in: Wolff/Brink (Hrsg.) (Fn. 25), Art. 22 DS-GVO, Rn. 3.
41 *Dammann*, in: Dammann/Simitis (Hrsg.), EU-DSRL, Baden-Baden 1997, Art. 15 EU-DSRL, Rn. 2.
42 *DEK* (Fn. 5), 24, 28.
43 *DEK* (Fn. 5), 28.
44 *DEK* (Fn. 5), 25 f.

https://doi.org/10.5771/9783748910770-289

V. Ausblick

Die Datenethikkommission ist mit ihrem Ansinnen, algorithmische Entscheidungsprozesse stärker zu regulieren, nicht allein. De lege ferenda finden sich verschiedenste Vorschläge, wie die Entscheidungsmacht von Maschinen über Art. 22 DS-GVO hinaus einer Regulierung zugeführt werden kann. Weitergehende Ansätze gehen etwa in Richtung einer Begründungspflicht für Algorithmen.[45] Vorgeschlagen werden nach dem Vorbild der Beipackzettel im Arzneimittelrecht umfangreiche Prüfungen und Informationen durch eine unabhängige staatliche Stelle.[46] Mitunter ist auch von einem „Algorithmus-TÜV"[47] die Rede. Heranziehen lassen sich auch Vorschläge für KI-Anwendungen wie etwa die Überprüfung mittels Audits durch unabhängige staatliche oder zertifizierte andere Stellen („qualifizierte Transparenz").[48] Gefordert werden zudem kontinuierliche Kontrollen; diese reichen von Kontrollalgorithmen über Risikomanagementsysteme bis hin zu Selbstregulierung und Haftungskonzepten.[49]

Last but not least können Lösungsansätze aber auch aus einer anderen – nicht ausschließlich rechtlichen – Perspektive betrachtet werden. Im Rahmen der KI beschäftigt sich beispielsweise der Forschungsbereich der „Explainable Artificial Intelligence" mit der Transparenz Künstlicher Intelligenz. Es wird sich jedoch erst zeigen müssen, ob und in welchem Rahmen die Forschungsergebnisse der erklärbaren KI den rechtlichen Anforderungen an eine Transparenz genügen.[50] Insofern müssen rechtliche Lösungsansätze in besonderem Maße die technischen Ergebnisse im Rahmen des Möglichen verstehen und einbeziehen. Kurzum, es bedarf also gerade einer interdisziplinären Herangehensweise, wie sie als Markenkern seit jeher auch das wissenschaftliche Wirken des Jubilars auszeichnet.

---

45 *Martini*, JZ 2017 (Fn. 16), 1020 f.

46 *Martini*, JZ 2017 (Fn. 16), 1020 f.; *Cech/Fischer/Human/Lopez/Wagner*, Dem AMS-Algorithmus fehlt der Beipackzettel, futurezone.at v. 3.10.2019.

47 *Dräger*, Ein TÜV für Algorithmen, Handelsblatt v. 21.8.2017.

48 *Molavi/Erbguth*, Einsatz maschinellen Lernens in der Justiz: Ethische und technische Aspekte, ITRB 2019, 160, 163.

49 *Martini*, JZ 2017 (Fn. 16), 1022 ff.

50 So für den Bereich der Verwaltung auch *Guckelberger*, Digitale Verwaltungsdienste für die Wirtschaft, GewArch 2019, 457, 462.

https://doi.org/10.5771/9783748910770-289